THE REGULATORY LANDSCAPE

OVERVIEW OF THE IMPACTS OF REGULATORY AGENCY PRACTICES ON CRITICAL INFRASTRUCTURE PROTECTION

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was prepared for the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. The report represents the opinions and conclusions solely of its developer, Argonne National Laboratory.

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the possible approaches and conclusions that were presented to the PCCIP for its consideration. The

series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

OVERVIEW OF THE IMPACTS OF REGULATORY AGENCY PRACTICES ON CRITICAL INFRASTRUCTURE PROTECTION

TABLE OF CONTENTS

OVERVIEW OF THE IMPACTS OF REGULATORY AGENCY PRACTICES ON CRITICAL INFRASTRUCTURE PROTECTION

1 INTRODUCTION

1.1 Purpose

The purpose of this study is to provide an understanding of the relationship between protection of critical infrastructure and the regulatory environment in which the infrastructure operates. This understanding will allow policy makers to target key areas in the search for solutions to the problem of assuring protection of our nation's critical infrastructures.

Specific objectives of this study are to:

- Provide a general overview of the regulatory practices of federal, state and local regulatory bodies that govern the operation of seven critical infrastructures;
- Identify current trends in regulatory reform as they affect critical infrastructures;
- Profile key representative agencies involved in developing and enforcing regulatory requirements in these seven areas;
- Analyze the effects of current regulatory schemes on critical infrastructure protection in the regulated industries; and
- Suggest approaches and measures to consider in developing regulatory measures for critical infrastructure protection.

1.2 Scope

The scope of this study is limited to seven of the critical infrastructures identified in Executive Order 13010: telecommunications, electrical power systems, gas and oil delivery and storage, banking and finance, transportation, water supply systems, and emergency services. Each of these infrastructures represents an industry that is subject to extensive regulation by federal, state and local agencies.

1.3 Organization of This Report

The remainder of this report is organized into eight sections. Section 2 provides an overview of the entire field of infrastructure regulation, identifying common themes and significant

distinctions among the different infrastructure sectors and their regulatory environments. Overall regulatory trends are highlighted, as well as recurrent themes that appear among the suggested measures for improvement. Sections 3 through 9 contain individual treatments of the infrastructures. For each infrastructure, the following items are provided:

- A "snapshot" overview of the current regulatory situation, covering the full regulatory field for that industry at the federal, state and local level.

- An analysis of regulatory trends at work. Most infrastructures have experienced considerable regulatory changes in the past two decades; the effects of these changes in some cases are still playing out.

- Detailed studies of a sample of regulatory agencies. For each infrastructure, a handful of regulatory agencies were selected for more detailed profiling, to provide a feel for how the regulatory system works in that industry. Selections were based on the following factors: (1) spanning the entire field of the infrastructure; (2) covering the spectrum of government levels (federal, state, local); (3) recognizing diversity of approaches; and (4) highlighting innovative or model approaches. For each agency profiled, there is a discussion of its regulatory jurisdiction, authority, and regulatory methods, and a summary of the pertinent regulations.

- An evaluation of the effect of regulatory practices on critical infrastructure protection. Elements of the regulatory systems that appear to enhance or detract from infrastructure assurance are identified. Examples of elements that enhance protection include direct security requirements, such as restricted access, background checks on employees, and emergency planning. Also included are requirements that are aimed at protecting the system against other hazards (e.g., harsh weather) but incidentally have the effect of reducing vulnerability against hostile action; for example, requirements for physical protection of equipment or system redundancy. Examples of elements that may *reduce* protection include requirements that force disclosure of sensitive information that hostile elements might use to identify vulnerable points.

- Suggested strategies to promote infrastructure assurance objectives through regulatory means. This section provides suggestions on strategies for enhancing critical infrastructure protection, without doing harm to the overall objectives of particular regulatory schemes. In light of the current trend toward deregulation, in many cases these strategies focus on cooperative industry standard setting, rather than development of traditional "command and control" regulations.

This report also includes an appendix listing relevant acronyms, agencies, associations and statutes.

2 OVERVIEW OF INFRASTRUCTURE REGULATION

2.1 The Regulatory Landscape

2.1.1 Historical Development of Infrastructure Regulation

Our critical infrastructure is the product of a long process of co-evolution between government and industry. Every aspect of the infrastructure, from its physical configuration down to patterns of ownership, reflects the influence of past and present government controls. These controls in turn originated in response to three main concerns: access to service, market power, and safety. These three issues cut across many different infrastructures.[1]

Access to Service

Promoting universal access to service has long been a feature of utility regulation, and is a stated goal of most utility-regulation statutes.[2] A prominent example of this policy was the establishment of a program of assistance to rural electric cooperatives under the Rural Electrification Act of 1936 (Pub. L. 74-605) for the express purpose of serving rural areas that might not otherwise be economic for utilities to serve. Similar policies have heavily shaped the development of the natural gas, telecommunications, and transportation industries.

Universal access has been perceived as a desirable social goal for several reasons: it provides the basis for economic growth, increases the standard of living, and generally brings the benefits of our social investment in infrastructure to the largest possible population. In addition, for some types of infrastructure, there is a positive feedback mechanism such that the more widespread the system is, the more useful it becomes. For example, as more people and businesses become reachable by telephone, the more valuable a telephone is. People come to rely on the telephone,

[1] For example, the Illinois Public Utilities Act provides for "adequate, efficient, reliable, environmentally safe and least-cost public utility services. . . ." (220 ILCS 5/1-102). The Communications Act of 1934 (48 Stat. 1064, as amended) established the Federal Communications Commission (FCC) "For the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States a rapid, efficient, Nation-wide, and world-wide wire and radio communication service, with adequate facilities at reasonable charges, for the purpose of the national defense, [and] for the purpose of promoting safety of life and property through the use of wire and radio communications . . ." (47 U.S.C. § 151).

[2] See footnote 1.

and the pressure on each household (and especially each business) to have one increases. Similarly, the more extensive the road system, the more valuable a car becomes as a means of getting places.

Market Power

Most of the infrastructures studied involve the transport of something such as electricity, gas, or water from a few production points, through main trunk lines, then through a very finely divided and extensive distribution network to individual users. Setting up such a system involves a huge capital investment, and in most cases also involves a delegation of governmental authority in order to condemn easements that spread across the landscape. The required investment in physical infrastructure creates a barrier to entering the market. On the one hand, no company would want to lay out such an investment without some assurance that it will pay off. On the other hand, once completed, the infrastructure investment puts the supplier in a position of power with respect to both customers and competition — to compete, another company would have to duplicate the delivery network. It would not be practical, nor desirable from a public policy standpoint, for another company to begin stringing wires or laying pipelines that are redundant with the existing network. But from the customers' standpoint, there is no choice but to deal with the company whose pipe, or wire, or railroad comes to town. The term "natural monopoly" was coined by economists to describe this situation.[3] Regulators have traditionally approached this situation by granting franchises to serve particular areas, thus assuring the company of demand, and at the same time regulating prices so as to protect the captive consumers from the effects of monopoly pricing.

Safety

Another factor that historically drove development of regulation is concern over safety. Power lines, pipelines, water supplies, railroads, airlines, etc. all carry the potential for disaster if not built, maintained and operated correctly. The community has an interest in ensuring that the companies performing these activities have the technical competence to manage their facilities in a safe manner. Thus, specifications for equipment, installation, operating practices, and employee qualifications became a common purview of infrastructure regulation.[4]

Banking and Financial Services

Regulation of banking and financial services has followed a somewhat different path and reflects different priorities than the regulatory systems sketched above. For one thing, it has a much

[3] See, for example, discussion of natural monopolies in Kenneth E. Train, *Optimal Regulation*, MIT Press, Cambridge, Massachusetts, 1991, pg.1 *et seq.*

[4] See, for example, the Illinois Gas Pipeline Safety Act, 220 ILCS 20/3(b): "Standards established under this Act may apply to the design, installation, inspection, testing, construction, extension, operation, replacement, and maintenance of pipeline facilities."

longer history: the government's role in banking long preceded the technologies that gave rise to the oil, gas, electric, and telecommunications industries. Also, the challenges posed by regulation of banking are substantially different than those associated with the other infrastructures. Regulation of banking and financial services is primarily aimed at (1) protecting depositors and investors; (2) providing a steady source of funds for investment in economic ventures; (3) maintaining a stable currency; and (4) providing an atmosphere of stability, trust and legal enforcement that will foster healthy economic growth. These goals are pursued through regulatory measures designed to ensure full and fair disclosure of information to investors, prevent banks and savings institutions from taking undue risks, and ensure the safety of deposited funds. The government also actively manages financial markets through control of interest rates and money supply, and through budgetary measures.

Emergency Services

Regulation of emergency services also differs significantly from regulation of the other infrastructures, since emergency services are primarily provided by governmental entities. A majority of emergency services are provided by local fire and police departments, public health services, and local medical services. The effectiveness of these organizations is subject to local political review and control rather than the pervasive, nationally based regulatory systems found in other infrastructures. With minor exceptions, only in the last couple of decades has the federal government established a major role in emergency planning and response.[5]

2.1.2 Current Trends in Regulation

All of the infrastructures have undergone major regulatory changes in recent years. The rationales underlying the original regulatory schemes have not been abandoned. However, in most of the infrastructures there have been major efforts to open markets and increase competition.[6] The major trends are summarized below.

Restructuring of Utilities

Starting in the 1970s, the traditional utility regulatory schemes began to be perceived as overly restrictive, stifling competition and in some cases causing artificial shortages of the commodities

[5] See discussion and notes regarding regulatory trends in Section 2.1.2.

[6] Although the historical goals of universal service and economics have not been explicitly disowned, some observers have pointed out that they conflict with the current emphasis on market competition. See, for example, Robert M.Frieden, *Dialing for Dollars: Should the FCC Regulate Interstate Telephony?*, 23 Rutgers Comp. & Tech. Law J. 47, note 16: "Presently, the universal service system is incompatible with the procompetitive efforts required by the Telecommunications Act . . . The current universal service system is a patchwork quilt of implicit and explicit subsidies. These subsidies are intended to promote telephone subscribership, yet they do so at the expense of deterring or distorting competition."

they were supposed to assure. A series of reforms was initiated, with the primary goal of increasing opportunities for competition and market forces to balance supply and demand. The reform process and its consequences are still playing out today. Although the reform process is commonly referred to as "deregulation," that is not an entirely accurate characterization. "Industry restructuring" is perhaps a more accurate term.

Industry restructuring refers to the fact that in many areas, including at least telecommunications, electricity, gas and oil, and rail transport, the effect of the recent changes has been to segment the industry into two or three parts. For example, AT&T divested its local telephone companies while retaining its long-distance service. The natural gas industry is being segmented into natural gas producers, interstate pipeline companies, and local distribution companies. Companies that were once "vertically integrated" from production facilities to ultimate consumers, are now broken up into separate units that either produce, transport, or distribute to individual customers. The purpose and effect of this restructuring has been to create separate markets for the bulk production and transport segments. Thus for example a large industrial consumer of natural gas is no longer tied to the local gas company; it can now purchase bulk quantities directly from a supplier and then contract with a pipeline company to have it transported to the factory.

This type of change puts suppliers and bulk transporters in the position of competing for business and lets market forces set prices, driving increases in efficiency and decreases in cost. Bulk pricing is in some sense deregulated. However, there is still a considerable regulatory presence. In fact, some transporters and local distributors might consider themselves to be less autonomous than before, in that they are now obliged to provide their services for the benefit of other corporate entities. For example, electric companies must now make their transmission lines available for other companies (their competitors) to send power to large customers (who were formerly *their* customers). Railroads must allow passage of competing shippers' freight over their tracks. Arrangements, procedures, liabilities, and rates for these transactions are still subject to regulatory control through the filing of tariffs.

Application of Risk Management Techniques

Under recent Congressional direction, some agencies are incorporating elements of risk management technique into their regulatory schemes. For example, the Accountable Pipelines Safety and Partnership Act of 1996 (Pub. L. 104-304) calls for the U.S. Department of Transportation (DOT) to perform risk assessments and cost-benefit analyses when setting pipeline safety standards. It also establishes a voluntary risk management demonstration program. Under this program, participating pipeline operators will have the opportunity to submit risk management plans designed to achieve an equivalent or greater overall level of safety (as compared with strict compliance with DOT standards) at lower cost. Another example is found in water monitoring. The U.S. Environmental Protection Agency (EPA) has proposed regulations for reform of chemical monitoring regulations under the Safe Drinking Water Act.

Under this proposed rule, drinking water suppliers would be able to tailor their monitoring programs to achieve the maximum safety benefit at the lowest cost, on the basis of risk analysis.[7]

Growth of Technological Emergency Response Capabilities

A major development in the regulation of emergency services has been the growth of specialized programs aimed at technological hazards. Governmental interest in this area was stimulated by technological disasters such as the nuclear power plant accidents at Three Mile Island and Chernobyl and the chemical releases at Bhopal, India and Institute, West Virginia. Subsequent regulatory action has included programs to promote radiological emergency preparedness at the state and local level,[8] a national hazardous material-response program,[9] a program to stimulate state and local hazardous material planning,[10] workplace safety rules for emergency responders,[11] and numerous requirements for emergency planning on the part of industrial firms handling hazardous materials.[12]

Reduction of Banking and Financial Service Restrictions

Recent changes in banking and financial service regulations have tended to reduce the degree of compartmentalization that had previously been imposed on the industry. By repealing part of the Glass-Steagall Act, Congress has allowed banks to grow larger and branch across state lines, subject to concentration limits, state laws, and evaluation of the companies. Further changes in the law allowed bank holding companies to own more than one kind of banking enterprise, so that small banks and mortgage lending institutions began to be combined under centralized regional management. However, such combinations are potentially subject to regulation by many agencies. In addition, banks are now permitted to offer types of financial services and investment opportunities that they previously could not.[13]

---

[7] U.S. EPA, *Drinking Water Monitoring Requirements for Certain Chemical Contaminants -- Chemical Monitoring Reform (CMR) and Permanent Monitoring Relief (PMR), Part II*, 62 FR 36100, July 3, 1997.

[8] See NRC regulations at 10 CFR 50, App. E and FEMA regulations at 44 CFR 350 *et seq.*

[9] National Contingency Plan, 40 CFR 300 *et seq.*

[10] 40 CFR 355.

[11] 29 CFR 1910.120(q).

[12] EPA regulations issued under the Resource Conservation and Recovery Act (RCRA) [applying to facilities that store or process hazardous waste (40 CFR 265.56)], Clean Air Act (CAA) [release prevention and response for hazardous air pollutants (40 CFR 68; 61 FR 31668, June 20, 1996; 61 FR 16958; and 61 FR 31730)], and Clean Water Act (CWA) [oil spill prevention and response (40 CFR 112)] all contain provisions addressing emergency preparedness.

[13] Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994 (Pub.L. 103-328, 108 Stat. 2338).

Regulation of the Internet

The Internet has experienced exponential growth, and is currently estimated to have at least several tens of millions of users worldwide. At the same time, the types of uses to which it is put are also multiplying. From the initial postal-like exchange of written messages and data, use of the Internet has diversified to include commercial transactions, advertising, financial transactions, and real-time audio and video transmission, among others. The Internet itself is rapidly becoming a vital part of our critical infrastructure.

Regulation of the Internet is still mostly at the discussion stage. Of the steps that have been taken, some have failed in the courts. However, it may be expected that the next several years will bring increased regulatory attention to at least certain types of Internet activities. A few such areas are outlined below.

- *Regulation of moral content.* Congress's attempt to sanction pornography on the Internet was declared unconstitutional by the Supreme Court in *Reno, Attorney General of the United States et al. v. American Civil Liberties Union et al.*, 117 S. Ct. 2329, June 26, 1997. In so doing, the Court identified First Amendment interests in Internet transmissions that will make it difficult to enforce regulations on the moral content of messages.

- *Telephony*. Given sufficient data transmission rates, users with appropriate equipment and software can use the Internet to conduct real-time audio exchanges; i.e. to mimic a telephone. Telephone service representatives have argued to the Federal Communications Commission (FCC) that Internet service providers performing this function should be subject to the same regulatory obligations imposed on telephone companies.[14]

- *Advertising*. Many home pages, particularly the popular search engines, are accompanied by advertising messages. Such advertising bears certain similarities to broadcast or print media advertisements; however, it differs in that the particular ad that appears to the user can be selected based on information about that particular user's preferences, patterns of Internet use, or demographic profile. Application of truth-in-advertising standards and other regulatory measures to Internet advertising has been approached differently by different jurisdictions.[15]

[14] See Frieden, *supra* note 6.

[15] As discussed by Dan L. Burk in *Federalism in Cyberspace*, 28 Conn. L. Rev. 1095 (Summer 1996), " Of course, even without the enactment of new laws or regulations, there are already on the books plenty of laws that states might apply to the Internet, including consumer protection statutes and other public law to police online behavior and commerce. The Minnesota Attorney General's office in particular has been very aggressive in pursuing what it considers to be online violations of Minnesota law, filing a flurry of lawsuits against out-of-state advertisers and service providers. The Illinois Attorney General's office is equally eager to get into the cyberspace game. By contrast, the Attorney General of Florida, has opined that because of the novel nature of the Net, forays into online enforcement of current law would be premature."

- *Commercial transactions.* As commerce on the Internet grows, regulations and legal norms will be developed to ensure that the system can be relied on, and that transactions will proceed according to a well understood set of expectations. As stated by one scholar,

> Businesses of all types routinely use the Internet for a variety of commercial transactions, and consumer services have begun to appear. At present, commercial traffic on the network generally culminates in an exchange of physical goods, and it is presently possible to access a variety of mailorder catalogs online, to arrange for purchase of music, books, fast food delivery, even flowers. Unlike transactions involving physical goods, delivery of digitized information products such as music, photographs, novels, motion pictures, multimedia works, and software can be accomplished entirely within the network itself. Such information products already represent a sizeable portion of the gross national product of developed nations. That portion is likely to increase world-wide, and the Internet will facilitate such increases. And, where there is commerce to be had, regulation is sure to follow.[16]

2.2 Opportunities for Enhancement of Infrastructure Security

2.2.1 Current Regulatory Requirements for Critical Infrastructure Protection

A survey of the regulatory environment for critical infrastructure reveals that there are relatively few instances where regulations directly address protection against hostile acts. Nuclear power plant operators are required to be prepared against a "design basis threat" described in some detail in terms of the numbers of persons involved, vehicles and weaponry at their disposal, types of expertise at their command, and cooperation by insiders.[17] These regulations make sense in the context of a nuclear power plant, where the consequences of an incident can be severe, the target is highly valuable and visible, and the facility is relatively defensible. The result is that nuclear power plants have multiple security perimeters, fencing, monitoring equipment, and round-the-clock security forces. Similar considerations and requirements apply, to varying degrees, at liquefied natural gas (LNG) storage facilities[18] and airports.[19] However, it is questionable whether this type of approach could be practically employed in other infrastructure contexts. Most elements of critical infrastructure are by their nature more spread out and less defensible than these facilities.

---

[16] *Id.*

[17] 10 CFR 73(a)(1).

[18] 49 CFR 193.2001 *et seq.*

[19] 14 CFR Part 107.

Many critical infrastructures are subject to regulatory requirements that have the effect of making the system more resistant to attack, even though they are aimed at reducing vulnerability to natural or accidental threats. For example, natural gas mains are required to be buried below ground. Burial protects them from ordinary threats such as storms or vehicle accidents; and it incidentally makes them less accessible to saboteurs. In fact, the more densely populated the area they go through, the deeper they are required to be buried. Similar examples are found in other infrastructures.

- Electrical substations are required to be fenced and locked, primarily to protect the public from accidental electrocution but also to prevent vandalism.

- Transmission line towers are built to exacting technical standards to prevent wind damage. Their robust construction also makes them generally more difficult to knock over, by whatever means.

- Certain types of protection are required for watersheds and surface water reservoirs that serve as drinking water supplies. These are primarily aimed at preventing contamination of drinking water supplies by pollution from runoff, migration from hazardous waste sites, or other types of conventional industrial pollution.

These and other standards that provide incidental protection from hostile acts are concerned exclusively with physical threats. Protection from cyber threats was not found to be addressed among the regulatory systems surveyed.

2.2.2 Proposals for Regulatory Measures to Enhance Infrastructure Protection

As noted, at present there are few regulatory measures directed at protection of critical infrastructures from hostile actions. Development of such measures will require careful review and analysis of costs, benefits, and options for achieving the desired level of assurance. Any proposal for regulatory action would have to be individually fitted into the existing regulatory system for that infrastructure. However, review of the current regulatory schemes for each infrastructure suggests a small number of themes that are common to multiple infrastructures — areas in which it may be worthwhile to seek regulatory solutions to problems of infrastructure protection. These recurrent themes are described below.

1. *Information protection*. In several areas, the operation of regulatory schemes causes information about the industry (e.g., schematic diagrams outlining networks of pipelines or power lines, or summaries of contingency planning) to be collected at a centralized location. Such concentrated information might be of interest to individuals intending to disrupt the system. Interviews with industry representatives indicated that they are concerned about this possibility. In one area — airport security — regulatory initiative has already been taken to impose controls over sensitive information.

2. *Contingency planning*. Most utilities, and certainly emergency services, already perform contingency planning to prepare for disasters. Such planning is generally supplemented by drills and exercises to hone response capabilities. However, preparedness efforts are based on responding to identified scenarios. The types of scenarios considered are often limited to natural disasters or technological problems of an accidental nature. Preparedness for malevolent acts could be enhanced by including that type of scenario among those considered in developing emergency plans.

3. *Preservation of redundancy*. In several industries, recent regulatory changes may reduce the level of redundancy in the infrastructure. As competition places greater premiums on economic efficiency, existing equipment is being used to capacity. There is more traffic on fewer lines. The result is less margin for dealing with disruptions to the system. Incentives for retaining reserve capacity could enhance the resiliency of infrastructure networks, possibly preventing small disturbances from being amplified into regional or national problems.

4. *Protection from cyber threats*. Reliance on computerized information systems is increasing. This trend is most pronounced in the telecommunications and banking areas, but is also present in all of the infrastructures in varying degrees. Electrical grids, oil and gas valves, and municipal water systems are all operated remotely by means of computerized data transmission. Security measures have been implemented in order to protect critical data and functions; however, there is little regulatory oversight of this area. There is a need for study in this area, to identify vulnerabilities, and determine for each infrastructure whether there may be an appropriate role for government-mandated or industry-based standards regarding cyber security.

2.2.3 Availability of Regulatory Leverage

In order to implement measures for infrastructure protection, it is necessary to have a mechanism for introducing new ideas or practices on a national scale. For some infrastructures, the regulatory field has a strong federal or coordinated industry presence that provides a convenient means for introducing new initiatives. In other areas, however, regulatory control is fragmented among many state and local jurisdictions, making it difficult to promulgate widespread change. For example, the EPA provides strong leadership in regulation of drinking water supply systems. Although most enforcement is conducted by states, they more or less uniformly adopt the EPA standards; any regulatory changes adopted by the EPA are soon echoed at the state level. Other aspects of water system regulation are covered by a set of industry-developed standards (promulgated by the American Water Works Association) that have been widely adopted by state agencies. Among electric utilities, the North American Electric Reliability Council, an industry organization, promulgates standards for contingency planning and operations that are uniformly followed. On the other hand, there does not appear to be any analogous forum in the oil industry. Although there is a substantial federal presence in oil industry regulation, it is split among several different agencies, and in fact much of the detailed control of production and safety standards takes place at the state level. It can be difficult to determine whose regulations apply to

certain particular pipes or valves. In considering opportunities for implementing change, it will be important for policy makers to consider what forums are available to disseminate their ideas to the industry.

3 INFORMATION AND TELECOMMUNICATIONS INFRASTRUCTURE

3.1 General Description of Regulation

3.1.1 Current Regulatory Environment

Federal regulation of wireline and wireless communication of voice, data, and image signals within the United States is authorized by the Communications Act of 1934 (the Act) (47 U.S.C.A. 47), as amended by the Telecommunications Act of 1996 (1996 Act) (Pub. L. 104-104, 110 Stat. 56). The Act established the Federal Communications Commission (FCC), as the body to execute and enforce its provisions.

With regard to national infrastructure policy, a role is also performed by the National Telecommunications and Information Administration (NTIA) which was created in 1970 within the U.S. Department of Commerce (DOC). Through its Office of Policy Analysis and Development, it plays the role of "principal advisor to the President on telecommunications policies."[20] As one of its primary policy functions, the NTIA was directed by Congress to foster "national safety and security, economic prosperity, and the delivery of critical social services through telecommunications."[21] The NTIA has filed numerous comments in matters docketed before the FCC to express the Administration's desires with regard to deregulation of the industry, particularly as to the assurance of universal access to telecommunications service at affordable rates.[22]

[20] 47 U.S.C.A. § 901(b)(6) and DOC World Wide Web home page, National Telecommunications and Information Administration, Office of Policy Analysis and Development, at http://www.ntia.doc.gov/opadhome/opadhome/html.

[21] 47 U.S.C.A. § 901(c).

[22] See, for example, Reply Comments of the National Telecommunications and Information Agency, May 30, 1996, *In the Matter of the Local Competition Provisions in the Telecommunications Act of 1996*, CC Docket No. 96-98.

In addition to the federal presence, all 50 states have some form of regulatory body that addresses telecommunications; generally it is a public utility commission (PUC) or a subpart thereof. For the most part, these state agencies are concerned with facility siting, equipment siting, and rate setting, but a growing number are addressing access and continuity of service.[23] They generally focus on promoting and accommodating commerce while ensuring the most democratic distribution of service economically permissible.

3.1.2 Current Trends in Regulation

At present, the information and telecommunications infrastructure is experiencing deregulation as a result of the 1996 Act. The primary objective of deregulation was to stimulate increased competition in the industry so as to ensure the lowest feasible service prices to individuals and businesses.

The stated intent of the 1996 Act was "to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies."[24] The deregulatory content of the 1996 Act opens markets by imposing new obligations for interconnection, unbundling of services, and resale of infrastructure access on existing providers of local exchange services.

Implementation of the provisions of the 1996 Act will require development of new business models for telecommunications to address costing and business practices in an industry that was previously highly oligopolistic. In recognition that local exchange markets will not immediately become competitive, Congress imposed immediate telemessaging and electronic publishing requirements on local exchange carriers aimed at detecting and preventing improper cost allocation, discrimination, or other anticompetitive conduct. The provisions of the 1996 Act are being implemented by the FCC through a series of hearings and subsequent orders.

Simultaneous with deregulation of the industry, there is a continuing and growing wave of new products and services being introduced. Emerging technologies such as synchronous optical networks, new wireless access with personal communications services, satellite nets, and advanced intelligent networks, when coupled with smaller, cheaper, and more powerful

---

[23] See, for example, (1) Illinois Code of Statutes, Chapter 220 (220 ILCS), 5/13-102; (2) *Implementing the Telecommunications Act '96*, Washington Utilities and Transportation Commission, summary of report findings, November 30, 1996; (3) California Public Utilities Code, Chapter 4, Article 8, Paragraphs 851-856 (Universal Service); (4) New Jersey Board of Public Utilities, Ratepayer Advocate Recommendations, Section V, *Definition of University Servic*e; (5) Public Utility Commission of Texas, Rule ¶23.97 relating to interconnection for local exchange service; (6) Report of the Public Utility Commission of Texas, references to universal, nondiscriminatory service as defined by the U.S. Telecommunications Act of 1996; and (7) *Texas Register* (20 TexReg 8777), October 24, 1995.

[24] See Telecommunications Act of 1996, P.L. 104-104, February 8, 1996.

computers, will change communication and information access in ways that are not yet fully clear. There will be a greater number of independent service providers, furnishing a greater variety of services and products to the end user, presumably at lower costs. This variety will make any systemwide security initiatives more difficult to develop and enforce. Each new technology will create additional challenges for regulators to balance service and security objectives.

In any communication system, there is a tradeoff between security and access. These conflicting goals are reflected in the statutes that set regulatory policy. For example, the principal objectives of the Act include service to "so far as possible . . . all the people of the United States." The Act also states as primary objectives the provision of communication services for the purposes of national defense and promoting safety of life and property. Most of the state statutes also contain language about the importance of both nondiscriminatory service and public safety. Resolving conflicts between the desire for a highly available, reliable, and affordable system for the general public, and the need for a secure, responsive, and reliable system for national security, law enforcement, and emergency response agencies will be a great challenge for the regulators.[25]

The greater part of the national telecommunications infrastructure is owned by private companies. These companies also possess the largest portion of the technical and operational expertise required to maintain the infrastructure. Federal and state regulators have long recognized these facts and have used the expertise of the system operating companies to help develop polices and regulations. The disaggregation of the industry brought about by the 1996 Act will bring in many new players at the local service level, with greatly varying degrees of expertise. Few if any of these new players will have the capital or expertise to address infrastructure assurance unless it directly relates to their service delivery. Any successful plan for accomplishing both the service and security objectives of the 1996 Act will require both (1) close coordination among the federal and state agencies involved and (2) the assumption of many of the tasks involved in managing the consequences of failure of infrastructure protection by the newly deaggregated telecommunications industry. Encouraging and embracing this industrial assumption of risk will involve a rethinking of traditional regulatory schemes, which have as one main tenet to keep individual service providers self-sufficient, and which discourage pooling of assets and activities.

[25] As was pointed out in an assessment of the impact of these technologies on military operations, " the characteristic that gives any system its potency — that the parts of a system enhance the effectiveness of one another — also make some systems susceptible to catastrophic failure if one of their central parts can be jeopardized." (Admiral William Owen, U.S.N. [retired], former Vice Chairman of the Joint Chief of Staffs, with Martin Libicki, in the introduction to *Dominant Battlespace Knowledge,* the National Defense University, Washington, D.C., 1995, pg. 11).

3.2 Description of Selected Regulatory Agencies

3.2.1 Selection Method

The FCC is the primary agency for federal regulation of the communications infrastructure. It is the principal interface between the federal government and the many public and private entities that make up the telecommunications industry. Even in areas where it does not exercise direct regulatory authority, the FCC is a "persuasive presence" promoting a coherent policy.

The state agencies selected for analysis represent various approaches to regulation of the telecommunications industry. They are among the states cited as exhibiting "leadership on the primary journey that will lead to the information superhighway."[26]

3.2.2 Agency Descriptions

3.2.2.1 Federal Communications Commission

Authority and Jurisdiction

The Act is the primary source of authority for the FCC. As stated in the Act, the jurisdiction of the FCC pertains to:

> all interstate and foreign communications by wire or radio and all interstate and foreign transmission of energy by radio, which originates and/or is received within the United States, and to all persons engaged within the United States in such communication or such transmission of energy by radio, and to the licensing and regulating of all radio stations. . .

The term "radio" has long since been interpreted to include all forms of transmission of electromagnetic energy for purposes of carrying information within the United States.[27] The FCC views its mission as being to "encourage competition in all communications markets and to protect the public interest."[28]

Techniques of Regulation

The FCC, like most regulatory bodies, has both quasi-legislative and quasi-judicial authority. It establishes and enforces administrative regulations but can also take testimony, subpoena

---

[26] *State Report on Citizen Participation*, Center for Policy Alternatives, Washington, D.C., August 1994.

[27] Mission statement, FCC home page at http://www.fcc.gov.

[28] Ibid.

witnesses and records, and issue decisions and orders. Although it has a direct investigative and enforcement capability, the principal regulatory technique used by the FCC is rulemaking, in which the provisions of applicable federal law are applied to a specific matter brought before the commission. The subject matter of a rulemaking may be a clarification or specification of the law for all parties[29]; establishment of a federal rule for governance of a particular part of the communication spectrum[30]; a ruling on a controversy concerning a regulated company or companies[31]; or any other matter that the FCC feels can be properly brought before it.

3.2.2.2 Other Federal Agencies and Departments

While the FCC has sole authority for regulating the interstate communications systems in the U.S., it is not alone in having responsibilities and duties that affect the operation and security of those systems. Within the federal criminal code, there are now provisions for investigation of fraud and related activity in connection with computers.[32] Among the "related activities" covered by this new statute are those computer crimes generally associated with the term "hacking," which result in threats to national security or financial damage to any person, corporate or real. This statute expanded the role of the Federal Bureau of Investigation (FBI), the U.S. Secret Service, and other federal and state law enforcement agencies with respect to investigating misuse of the national information infrastructure. In addition to these civilian agencies, the U.S. Department of Defense (DOD) has become more active in the last five years in investigating computer crimes involving defense property and personnel.

3.2.2.3 California Public Utilities Commission

Authority and Jurisdiction

The California Public Utilities Code (CPUC) (CalStat, Title 70 *et seq.*) is the foundation of regulation in California. The CPUC was developed from the Railroad Commission Amendment of 1911, establishing a constitutionally mandated Railroad Commission, which became the California Public Utilities Commission (the Commission) in 1946.

The jurisdiction of the Commission has long since been extended generally to water, waste disposal, electrical generation and service, natural gas, and all forms of transportation. Under the

---

[29] Op. cit., *In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996*.

[30] For example, FO Docket No. 91-171/91-301, FCC 94-288, establishing portions of 47 CFR Parts 0, 11, 73, and 76.

[31] For example, DA Docket No. 97-1019, *In the Matter of Bellsouth Cellular and GTE Wireless, and AT&T Wireless Services, Inc*.

[32] 18 U.S.C.A. §1030.

CPUC, the Commission has broad powers to regulate safety, standards of service, and rates in regulated industries. Part 2, Chapter 10, of the CPUC, entitled "Telephone Corporations," gives the Commission authority to regulate telephone service and equipment.

Techniques of Regulation

The five commissioners, who make all policy, procedural, and rulemaking decisions, are appointed by the governor of California, with the advise and consent of the state senate, for staggered six-year terms. The Commission has quasi-legislative and quasi-judicial powers over regulated companies. The guiding principal for the Commission is to "benefit ratepayers through lower rates, new and improved utility products and services, and protect consumers where competition otherwise does not."[33] In meeting this objective, the Commission "balances the public interest and need for reliable, safe utility services at reasonable rates with the need to assure that utilities operate efficiently, remain financially viable, and provide their stockholders with an opportunity to earn a fair return on investment."

The Commission has a Telecommunications Division, composed of three branches responsible for advocacy, advisory, and compliance activities. These branches and their specific responsibilities are as follows:

- The Carrier Branch is responsible for processing tariffs of local exchange carriers, competitive local carriers, nondominant interexchange carriers, and wireless service providers. Thus this branch oversees price setting for all local commercial companies that provide telecommunications services to the public. The Carrier Branch also enforces compliance with Commission decisions and with service and reliability standards. In addition, it reviews general orders of the Commission to ensure that they reflect the competitive environment and changing regulatory structure for the telecommunications industry.

- The Market Structure Branch is responsible for implementation and oversight of Commission rulings regarding local competitive issues. This Branch reviews, analyzes, and advises the Commission about carrier-to-carrier arrangements and interconnecting agreements, competitive costing, pricing, and unbundling of services. This Branch also reviews utility applications for mergers, divestitures, and acquisitions.

- The Public Programs Branch is responsible for oversight and implementation of special issue programs (such as those for the disabled, elderly, and bedridden), service assurance for the needy, and pay telephones. This Branch also develops and implements consumer protection and education programs, and it reviews, analyzes, and implements the Universal Service program for California.

[33] Unless otherwise noted, all quotes in this section are from "About the CPUC," at ftp.cpuc.ca.gov.

The Commission has also formed a federal/state legislative team to actively coordinate responses to legislation and proposed legislation.

3.2.2.4 Illinois Commerce Commission

Authority and Jurisdiction

The Illinois Public Utilities Act lays out the structure and authority for regulation of telephone public utilities in Illinois (220 ILCS 5/1-101 *et seq.*). Under the Act, the Illinois Commerce Commission (the Commission) has a general mandate to assure safe and efficient operation of utilities and has powers to investigate accidents and enforce administrative orders related to safety equipment and practices. In general, however, the Commission's authority focuses on financial and economic matters, including rate setting, rather than public health and safety. The Commission determines acceptable rates and charges on the basis of a prescribed formula and a hearing process. The Commission has issued rules and regulations concerning the rate-setting process and other aspects of its oversight of utilities.

The Commission is responsible for general supervision of all public utilities and is authorized to inquire into the management of such utilities and to keep itself informed as to the manner and method in which the utilities' business is conducted.[34] This supervision covers the utilities' general condition, capitalization, and the manner in which their plant, equipment, and other property is managed, conducted, and operated. The Commission is responsible for ensuring that utilities provide adequate, reliable service and otherwise comply with the Illinois Public Utilities Act. However, the Act specifically limits the Commission's authority so as not to overlap with that of other agencies. The Commission may not enforce requirements that are vested in another entity.

Every public utility must obtain a certificate of public convenience and necessity from the Commission before transacting business within the state or beginning any construction of any new plant, equipment, property, or facility. A certificate will be issued only if the public utility demonstrates that the proposed construction is necessary to provide adequate, reliable, and efficient service to its customers. Every public utility must furnish to the Commission any information required by the Commission, including maps, profiles, reports, documents, books, account, papers, and records that in any way relate to its property or affect its business, and inventories of its property.

[34] A public utility is defined as anyone that owns, controls, operates, or manages, within the State of Illinois, directly or indirectly, for public use, any plant, equipment, or property used or to be used for, or in connection with, the production, storage, transmission, sale, delivery , or furnishing of heat, cold, power, electricity, water, or light, except for those public utilities owned or operated by any political subdivision, public institute of higher education, or municipal corporation of the state. The definition of public utilities also does not include water companies that are purely mutual concerns having no rates or charges for service but that pay the operating expenses by assessment upon the members of such a company and no other person.

The Commission is authorized to conduct management audits or investigations of utilities if necessary. Upon complaint or during a rate proceeding, the Commission may investigate claims of poor service and reliability, but generally only in connection with fiscal responsibility and to determine the return on investment the company may receive in its rates. Claims for damages resulting from service outages, or other cases where a public utility has failed to comply with any provision of the Illinois Public Utilities Act or any rule, regulation, order, or decision of the Commission, are not within the jurisdiction of the Commission and must be brought in the Illinois Circuit Court.

The Commission also has the authority to investigate all accidents involving utility property or activities that result in loss of life or injury to a person or property. The Commission then has the authority to issue orders or recommendations to the utility concerning the accident circumstances. This provision is rarely used. If the Commission determines, after hearing, that the practices, equipment, or service of any public utility, or the methods of distribution, storage, or supply employed by the public utility are unsafe, improper, inadequate, or insufficient, the Commission may issue an administrative order, decision, rule, or regulation requiring corrective action by the utility.

The Commission can issue administrative orders to require public utilities to comply with the Illinois Public Utilities Act or any rule, regulation, or order issued by the Commission. If the utility does not comply with such order, the Commission may file an action or proceeding in the appropriate Illinois circuit court. Any public utility or other corporation, that fails to comply with the provisions of the Illinois Public Utilities Act or Commission rules, regulations, or orders is subject to a civil penalty of not less than $500 nor more than $2,000 for each and every offense. Every person who fails to comply with the provisions of the Illinois Public Utilities Act or any order, rule, or regulation of the Commission is also guilty of a Class A misdemeanor.

The Commission has additional responsibilities for regulation of "telecommunications rates and services" under the Universal Telephone Service Protection Law of 1985 (which amended the Illinois Public Utilities Act, 220 ILCS 5/13-100). The duties of the Commission in this regard, as set out in 5/13-301 *et seq*., are to participate in all federal programs intended to preserve or extend and monitor universal service. The authorities and powers of the Commission under the Illinois Public Utilities Act, such as issuing certificates of service authority, establishing rates and charges, and conducting general oversight, are applicable to all noncompetitive telecommunications services. Certain sections of the above law also apply to competitive telecommunications rates and services. System security issues are not addressed in this portion of the Illinois law; however, the Telecommunications Facility Fire and Emergency Act (220 ILCS 45/0.01 *et seq*.) requires appropriate measures to prevent major interruptions of telecommunications services. The implementing regulations for this Act are discussed below in Section 3.3.1.

Also of particular interest in the context of the information and telecommunications infrastructure, 5/4-201 of Chapter 220 states that:

> It shall be the duty of the Commission, at the direction and discretion of the Chairman, to assemble and maintain an electronic trespass enforcement assistance staff consisting of experts in computer systems, electronics, and other professional disciplines to aid public utilities, businesses, individuals, and law enforcement agencies in detecting and preventing electronic trespass violations and enforcing the provisions of Section 16-9 of the "Criminal Code of 1961," approved July 28, 1961, as amended or any other relevant statute.

This provision has not been implemented. The Commission has, however, been very active with the Office of the Attorney General in developing the Illinois Commission on Electronic Commerce (ICEC) and the resultant draft Illinois Electronic Writing and Signature Act. At present, the focus of the ICEC and the draft legislation is to further the commercial use of emerging electronic media by legally defining documents, records, and signatures in their electronic form and by specifying how and under what conditions such electronic versions of legal instruments can be used in place of their physical counterparts and how the public can be protected when it relies on such electronic instruments.

Techniques of Regulation

The Commission carries out its duties through (1) hearings to determine compliance with applicable laws and its own rules, (2) publication of reports on the status of the regulated industries, and (3) rate setting procedures for all providers of regulated services in the state. The Commission also conducts and publishes studies on a variety of subjects as directed by the Illinois General Assembly. For the purposes of this report, the most pertinent of these studies are those concerned with the classification of new services and with the implications of regulating multiple certificates of service authority for intermarket service areas and local exchange services. It is in these areas of local service delivery where the emphasis on ensuring universal service and unbundled services will have the greatest impact on infrastructure protection. New technologies are being rapidly introduced into telecommunications, often in the form of new services. If a narrow view of classification of services is taken, complications in providing adequate measures of security will increase. For example, a regulatory viewpoint that fails to accommodate the convergence of video, information delivery and processing, communication, and entertainment product delivery will not have the scope necessary to correctly address system reliability and performance.

3.2.2.5 New Jersey Board of Public Utilities

Authority and Jurisdiction

The New Jersey Board of Public Utilities (NJBPU or the Board) was put in place by then-Governor Woodrow Wilson in 1911 for the purpose of setting rates, approving financing, and setting service standards for all regulated industries. The agency is autonomous in its decision making with regard to the energy, transportation, commercial, and consumer services and telecommunications industries that it regulates.

The Board is in the process of completing a reorganization plan begun in 1995. The reorganization is intended to increase the efficiency of its operations while emphasizing consumer issues such as affordability of service, safety, reliability, and economic issues such as maintaining the value of shareholder investment in utility companies.

As prescribed in New Jersey law, the duties and authority of the NJBPU are to:

1. Maintain universal telecommunications service at affordable rates;

2. Ensure that customers pay only reasonable charges for local exchange telecommunications services, which shall be available on a nondiscriminatory basis;

3. Ensure that rates for noncompetitive telecommunication services do not subsidize the competitive ventures of providers of telecommunications service; and

4. Provide diversity in the supply of telecommunications services and products in telecommunications markets throughout the state.

The law also gives the NJBPU the authority to approve alternative forms of regulation in order to address changes in technology and the structure of the telecommunications industry, modify the regulation of competitive services, and promote economic development.[35]

Nowhere in the Title 48 is system security or protection addressed. Section 2-23, entitled *Safe, Adequate Service*, states that the Board can require a utility to provide such service but limits the objective of such a requirement to environmental protection.

Techniques of Regulation

The NJBPU carries out its duties principally by means of hearings and rulemaking focused on rate setting, tax policy for utility services, industry restructuring, stranded assets, expanding

[35] New Jersey Permanent Statutes, Title 48.

competition, and economic development. There are no records available of any hearings held or studies made by the Board with specific regard to infrastructure reliability or protection.

3.2.2.6 Public Utility Commission of Texas

Authority and Jurisdiction

In 1995, the legislature of Texas adopted a new Public Utility Regulatory Act (PURA95), which directed a substantial reorganization of the Public Utility Commission of Texas (PUCT or the Commission). The Commission as reestablished consists of three commissioners, appointed by the governor for staggered, six-year terms, with the advise and consent of the state senate. The powers and duties of the PUCT include establishing "a comprehensive regulatory system which is adequate to the task of regulating public utilities . . . to assure rates, operations, and services which are just and reasonable to the consumers and to the utilities."

Under PURA95, the jurisdiction of the PUCT is limited to regulation of electrical energy (Title II) and telecommunications (Title III). Within that context, the PUCT is given significant authority to carry out the objectives of PURA95 with regard to enhancing competition in local service. For example, the provisions of §§1.101, 3.001, 3.051, and 3.458 would appear to give the Commission jurisdiction to require all holders of certificates of convenience and necessity to actively work toward redundant interconnection. PURA95 does not make any specific reference to system security or infrastructure protection. The Commission has adopted a policy of monitoring industry compliance with FCC orders with regard to priority of restoration of service after an interruption. The PUCT *Emergency Procedures for Telephone Utilities* requires local exchange companies to report service outages of four hours or more that affect:

- 50% of the toll circuits serving an exchange,
- 50% of the extended area service circuits serving an exchange,
- 50% of a central office, or
- 20% or more of an exchange's wire center access lines.

These procedures also require that in the event of a major emergency (e.g., loss of major portions of local service due to fire, floods, hurricanes, freezing, sabotage, or war), the PUCT is to be notified as soon as possible. However, according to a respondent at the PUCT staff, no specific state response plan standards have been established by the PUCT. The PUCT is relying on the industry to meet emergency response needs by reliability standards and the return-to-service prioritization determined under federal guidelines. The Commission has appointed one of its members to represent Texas on the National Network Reliability Council.

Techniques of Regulation

Under the PURA95, the PUCT carries out its responsibilities principally through the ratemaking process. The PUCT uses economic incentives to gain its objectives of quality and reliability of service, universal availability, and financial stability for the industry. System security has not been a stated objective for the ratemaking process. The PUCT is required to report periodically to the state legislature on a variety of subjects. Infrastructure protection is not included in any of these reports. PUCT staff indicated that assessing and addressing security and infrastructure protection are implicitly made the responsibilities of the industry, not the PUCT.

3.3 Regulations and Critical Infrastructure Protection

3.3.1 Impact of Regulations on Critical Infrastructure Protection

Threats to Information and Communications Infrastructure

To assess the impacts of regulations on information and communications infrastructure assurance, it is necessary to characterize the types of threats being considered. Appropriate protective measures may depend on the type of threat contemplated, although some measures may be common to all threats. Threats to information and communications may be divided into three types:

1. *System destruction*. Hostile elements might attempt to destroy a data bank or communication system so that it cannot be used at all (e.g., bring down a local [big city] telephone network or long distance service). This type of threat might involve either physical assault (e.g. bombing a key facility) or cyber attack.

2. *Corruption or destruction of data (cyber threat)*. Hostile elements might attempt to corrupt or delete information in key systems. For example, they might try to disrupt banking, commerce, or utilities by "hacking" into particular systems and introducing false or misleading data, deleting data, or deliberately manipulating the system in certain ways (e.g., turning off power grids or disrupting market trading)
3. *Unauthorized access to information*. Hostile elements might attempt to use information systems to obtain data that is classified, proprietary, or "private" in the personal sense. While potentially harmful, such actions fall more appropriately under the category of national or industrial espionage rather than terrorism.
4. *Theft of service.*

5. *Service abuse*.

Discussions of information security may focus on one type of threat or encompass all of them. "Access" to a computer system is often discussed, on the basis of the assumption that it may lead to any on of the three consequences above.

Impacts of Current Regulations

As indicated by the sample of regulatory agencies discussed in Section 3.2, few regulations directly address information and communication system security. At the federal level, there are criminal sanctions for tampering with the Public Switched Network (PSN) and national security information. These penal statutes promote system protection by deterring some who would intentionally tamper with the PSN.

Law enforcement agencies, intelligence agencies, and the military all have specific regulations regarding operational security (OPSEC), system security (SYSEC), and information security (INFOSEC). However, these regulations address only data and systems under the direct control of the government and only indirectly affect security standards for the PSN.

Apart from standards for systems used by the government and those directly related to national security, the development of standards that specify protection of data is in its infancy. Current regulations emphasize system reliability rather than system protection. To a significant degree, all of the equipment standards, frequency separation specifications, and reliability measures do affect system security, but only tangentially.

At the state level, the regulatory bodies focus primarily on economic considerations. State regulators are principally concerned with consumer protection and investor confidence. They must ensure that telecommunications service is available to the greatest number of people for whom such service can be economically provided. Additionally, they must ensure that investors in utility securities have confidence in the health of their utilities and will thus accept favorable interest rates on the bonds and debentures that must be sold to finance the needed infrastructure. Security *per se* has not been a major concern. A notable exception is the State of Illinois, which adopted security requirements for telephone switching stations after an accidental fire caused a significant disruption of service.

A fire at a switching facility in Hinsdale, Illinois, resulted in a serious, extended loss of telephone service over a large suburban area. In response, the Illinois Commerce Commission, in conjunction with the Office of the State Fire Marshal and the Illinois Emergency Management Agency, promulgated special rules for telephone utilities (83 IAC 785). These rules require all switching facilities to have physical security in the form of a door lock, card control entry, or security guard to prevent unauthorized entry or malicious disruption of service. Each facility must have a lock box system to facilitate access to the telecommunications equipment during an emergency situation. Each telephone utility must develop procedures providing for the continued operation of its services in the event of natural or human-caused disasters, including priority restoration of critical services such as police, fire departments, hospitals, and 911 service. In addition, each utility must notify the Illinois Emergency Management Agency of any major service outage expected to last 12 hours or more. Each switching facility must have a direct alarm monitoring communication channel to a fire department. All electrical service to switching facilities must meet fire code requirements.

In addition, the ICC requires central offices to have a reserve battery supply of five hours in locations where emergency power generators are not installed and three hours where they are. In central offices that have more than 3,000 working lines, a permanent power generator must be installed. There are also requirements to ensure that emergency systems (911 service) are not interrupted, which include physical security for all vital equipment to prevent malicious disruption of service, and wherever practical, underground service entrances for electric and telephone service.

Effect of Deregulation and Technical Change

In the last decade, there have been a great multiplication of information and communication services, brought about partly through industry deregulation and partly through the development of many new technologies and products. The popularization of cell phones, cable television, satellite communications, home computers, the Internet, distributed computer networks, electronic banking, and many other products and services has greatly increased the role of the information and communications industry in business and personal life. This trend is anticipated to continue for at least the next decade as well.

In the communications industry, one result of this trend may be an increase in the natural resiliency of the infrastructure. Twenty-five years ago, essentially all general-purpose personal and business communications were conducted via a single company's network. This system worked well and incorporated some redundancy and safeguards against breakdown. However, it is far different from the current situation, in which multiple long-distance providers have independent trunk networks, cellular telephones, and widespread access to the Internet. There are now many more ways to get a message from point A to point B. In addition, local telephone service is currently being deregulated, and it is anticipated that this will lead to further redundancy in local networks, as independent local nets and switching equipment are installed. In this respect, the information and communications industry may differ from other infrastructures (such as gas distribution or rail transport), where deregulation appears to be leading to decreased capacity margins and reductions in the physical redundancy of the system.

Another effect of the current regulatory climate is that protection of information and communications is a major private-sector activity, undertaken by commercial and industrial firms. Firms performing information-intensive work have developed methods of data protection and transmission to ensure privacy and have a reservoir of expertise in this area. There are tremendous business incentives to protect vital information, and the market has responded with methods and equipment for doing so. All this has occurred without benefit of regulatory intervention or standards.

3.3.2 Measures for Improvement

Governmental Recommendations

A number of federal-level groups have been studying information and communications security and have developed recommendations on how to proceed. The National Communications System (NCS)[36] has recommended further study to identify and characterize the nature of the threat to our national information infrastructure. In addition, the NCS has recommended that government and industry cooperate to develop:

- Protocols for industry-government information exchange regarding threats and risk;
- Protocols and mechanisms for information protection that are cost-effective and will not unduly impede communications;
- Statutes and regulations to implement such protocols, as needed; and
- Priorities for investment in infrastructure to reduce vulnerability.

The Network Reliability and Interoperability Council (NRIC), an FCC-chartered group, has studied telecommunications network accessibility and security. This group warns that "without a full range of security measures in place, both systems and data are in danger of misuse, corruption, and loss of confidentiality."[37] The NRIC has developed recommendations on government-industry cooperation that are somewhat similar to the NCS recommendations. In addition, the NRIC has recommended expansion of reporting requirements for outages and suspected attempts at intrusion. In interviews, members of the NRIC and FCC staff expressed concern that the reporting standards for outages affecting especially important classes of service such as major airports, military installations, government facilities, nuclear power plants, and 911 special facilities[38] were not rigorous enough for the growing complexity of the system. There was a strong consensus that an improved automated reporting system, with a greater ability to discriminate among kinds of system interferences and outages, was needed. Such a system would need to be augmented with regulatory language requiring additional and more finely focused data capture. Changes of this kind are unlikely to occur if left strictly to the competitive pressures of a deregulated industry.

The NTIA has focused on protection of personal information. The NTIA has recommended that

[36] The NCS was established in 1963 to provide oversight of systems to support critical diplomatic, military, and intelligence communication. It has assumed a prominent place in discussions of current vulnerabilities of the national communications and information infrastructure.

[37] NRIC Focus Group 1, item 3.01.01.04, opened 2/18/97.

[38] 47 CFR 63.100.

national standards be developed for the collection, use, and disclosure of telecommunications-related personal information. Such information includes personal telephone numbers and addresses linked in databases with employment, age, income level, marital status, purchasing habits, health records, and other highly personal data.

Industry Perspective

Interviews with numerous industry executives, cited throughout this section, have shown that the industry is quite cognizant of the need for infrastructure protection. System security is considered vital to the industry's economic interests. However, members of the industry are wary of federal regulation. They consider themselves to be the appropriate entities to address system security issues. They favor innovative and energetic development of new "best practices" (which are industrywide methods of dealing with operational security and reliability issues) and "standards" (which are industrywide technical requirements for dealing with functional performance issues). Representatives of both established carriers and new entrants see the need for incentives that will bring them together in a community of interest to develop standards and best practices.

Recommended Actions

The rate of technological change in the information and communications industry makes it necessary to adopt new approaches to regulation. If federal and state regulators follow the traditional process of hearings, followed by promulgation of rules, followed by amendment of the rules to adjust to emerging needs, they may be caught in a control loop in which their actions will lag behind reality to such a degree as to be ineffective or even harmful.[39] Instead of the usual top-down regulatory approach, the opportunity presented by the 1996 Act should be used to facilitate standard setting on the part of industry. This effort will involve (1) permitting firms to cooperate on security measures without fear of antitrust prosecution and (2) punishing those who abuse the cooperative nature of the system as a means to circumvent competition.

The appropriate roles for the government to take in protecting the emerging telecommunications and information infrastructure are as follows. First, it must articulate a clear statement of the priority of such protection over the competing goals of fostering competition, growth, and universal service. Second, it must establish criteria that target public and private development of solutions to technical issues in infrastructure assurance. Third, it must provide a mechanism through which the stakeholders in the infrastructure can exchange information about the nature and extent of threats to the infrastructure.

---

[39] The FCC has always relied on the industry for technical support in crafting federal rules and guidelines. As long as there were relatively few members in the industry and the industry members could stay ahead of the introduction of new technologies that altered the regulatory landscape, there was adequate "slack" in the process to allow thoughtful development of these national rules and guidelines. Both the pace of change and the increasing number of actors have made this process very difficult to manage.

In developing a national policy that addresses both physical and cyber security, the FCC is the best candidate to act as convener of the community of interest. However, the objective should not be codification of the resulting policy into agency rules, which would then need to be under constant review and amendment. To provide the appropriate guidance with flexibility, the most promising approach is to create a government-industry council, modeled after the NRIC[40] and charged with addressing infrastructure protection issues. This group would be responsible for integrating the recommendations of the federal, state, and industry into measures for improvement, such as best practices, standards, and research and development objectives. The forum body should be organized and staffed so that its activities are ongoing and continuous, with the statements and objectives constantly under review.

Such a council should view its purpose as developing policies aimed at providing the greatest degree of choice among telecommunications services and products, to the greatest number of people possible, with the greatest degree of security and reliability that is technically and economically feasible. This is not an easy task, but it can be done if the federal government regards issuance of rules and regulations as a recourse of last resort, to be used only when community development of standards, statements of best practice, and research objectives prove to be unwieldy, unreliable, or unproductive.

[40] See a similar quasi-regulatory structure and function in the discussions of the role of the North American Electric Reliability Council (NERC) for the electric industry in Sections 4.1.1 and 4.3.1.

[This page intentionally left blank.]

4 ELECTRIC INFRASTRUCTURE

4.1 General Description of Regulation

4.1.1 Current Regulatory Environment

Industry Overview

The U.S. electrical infrastructure is designed and operated to provide electrical power to industrial, commercial, and residential customers. It is composed of power generating facilities, high-voltage bulk power transmission lines that carry power over long distances, substations that "step down" the voltage for local distribution, and local distribution networks that carry the power to end users. At the level of generating and bulk transmission, the facilities are interconnected to form networks. Electricity generation and distribution are actively managed (in real time) on a regional basis to maintain an even supply of power to all users.

The majority of the U.S. bulk power system has evolved into three major networks (power grids), which include smaller groupings or power pools. The major networks consist of extra-high-voltage connections between individual utilities designed to permit the transfer of electrical energy from one part of the network to another and between one utility and another. These transfers rely on contractual arrangements and adequate transmission capacity. The three networks are (1) the Eastern Interconnected System, consisting of the eastern two-thirds of the United States (to the Rocky Mountains); (2) the Western Interconnected System, consisting primarily of the Southwest and areas west of the Rocky Mountains; and (3) the Texas Interconnected System, consisting of a significant portion of Texas. The Texas Interconnect is not interconnected with the other two networks (except for certain direct-current lines). The Eastern and Western Interconnects have limited connections to each other. The Eastern and Western Interconnects are completely integrated with most of Canada and have links to the Quebec Province power grid. The Western and Texas Interconnects are linked with different parts of Mexico.

The business units that make up the electrical infrastructure include public, private, and cooperative entities. The ownership structure of this infrastructure is in part the result of past and present federal programs. For example, the Rural Electrification Act of 1936 (Pub. L. 74-605) set up the mechanism for creating rural electric cooperatives. Rural cooperatives are consumer-owned and operated nonprofit utilities. They operate only in rural areas and are generally unregulated for the production and transmission of electricity within their own territories. These rural cooperatives can be small concerns serving a farming community or can be large companies providing electric service to consumers in several states. The federal government also has established a number of power administrations that generate and sell electricity. Federal generating facilities are normally hydroelectric dams, but the Tennessee Valley Authority (TVA)

also operates other types of power plants. In addition to the federal power administrations, there are numerous state and local government power systems, primarily municipal systems. Some of these do not generate their own power but instead purchase it from another utility and perform only local distribution. The remainder of the infrastructure is owned and operated by investor-owned utilities. Investor-owned utilities constitute the majority of the infrastructure. The business structure of these entities has been shaped by legal constraints. The Public Utility Holding Company Act of 1935 (PUHCA) (15 U.S.C.A. §§ 79-79z), enacted to eliminate holding company abuses, required them to be composed of a single integrated public utility system located in and serving a single geographic area.

Overview of Current Regulatory Scheme

Electric utilities are regulated by both federal and state agencies. The Federal Energy Regulatory Commission (FERC) regulates the interstate wholesale transmission and sale of electricity, and issues construction permits for power plants and transmission facilities.[41] This permitting process takes into consideration both the public need and the utility's ability to meet public demand for electricity and comply with all applicable state and federal regulations. These permits are issued in the form of FERC Orders, which are enforceable in the U.S. district court of appropriate jurisdiction. FERC also exercises its economic regulation of electric utilities through approval of electricity rates and corporate structure (18 CFR 35). FERC has the authority to order interconnections between utilities when it is determined to be for the public good (18 CFR 32).[42] FERC also exercises plenary policy-setting authority through the issuance of general orders. A recent example is the orders implementing wholesale market deregulation (FERC Orders 888 and 889). Those orders are discussed in more detail below.

State public utility commissions (PUCs) have jurisdiction over the intrastate retail sale of electricity. Usually, a state PUC must issue a permit, license, or certificate to an electric utility before it can begin construction and operation of a generating facility or transmission line. This permitting process is economic in nature and usually involves a determination that there is a public need for the electricity to be generated and that construction of the plant is a prudent investment by the utility. The order may set out specific directions concerning the financing of the construction and the treatment of the completed plant and the related construction expenses in the utility's ratemaking dockets. The order may require that certain construction standards and operational procedures be followed.[43] Many states regulate the erection of transmission lines, including the height, tower construction, and spacing of the lines along the utility's easement. In

[41] Federal Power Act, 16 U.S.C.A. §791 et seq., and implementing regulations at 18 CFR Part 4.

[42] The Department of Energy (DOE) also has authority (under § 202(c) of the FPA) to order temporary interconnections between electric utilities during emergency situations such as unexpected outages or breakdowns of facilities.

[43] Except for nuclear power plants, which receive a separate license from the U.S. Nuclear Regulatory Commission (NRC) and comply with NRC construction standards and operational procedures.

some cases, municipalities may have additional regulations that must be met in erecting or burying electrical distribution lines within the city limits.

Utilities with nuclear power plants are also under the jurisdiction of the U.S. Nuclear Regulatory Commission (NRC). The Atomic Energy Act of 1954 (42 U.S.C.A. §§ 2011-2296) authorizes the NRC to regulate the safety aspects of the construction and operation of nuclear power plants.[44] The NRC promulgates regulations, issues construction and operation licenses, maintains on-site inspection teams, and issues enforcement actions when license conditions or its regulations are violated.

Although not a regulatory body, a major player in electric reliability is the North American Electric Reliability Council (NERC). NERC is a voluntary association of utilities formed in 1968 in response to the Northeast blackout of 1965. NERC's mission is to promote the reliability of the electric supply for North America by reviewing lessons learned; monitoring the existing system for compliance with NERC policies, standards, principles, and guidelines; and establishing forward-looking policies, standards, principles, and guidelines to assure the future reliability of bulk power systems. NERC is proactive in assuring continued reliability of the power system. As discussed below, despite the presence of federal and state regulatory bodies, NERC has become the major influence on electric system security.

4.1.2 Current Trends in Regulation

Federal regulation of electric utilities dates back to 1935, with the enactment of PUHCA and the FPA. The Federal Power Commission (FPC) was created to oversee interstate transmission and wholesale of electricity. Its authority was later transferred to FERC.

The recent changes to electric industry regulation started with the Public Utility Regulatory Policies Act of 1978 (PURPA). Passed in response to uncertainty in the energy market in the 1970s, it allowed nonutility facilities to generate and sell electricity on the wholesale market. These qualifying facilities (QFs), either cogenerators or small power producers, sell their excess energy to public utilities pursuant to contracts that by law set the rate at the purchasing utility's "avoided cost." QFs are exempt from rate and accounting regulation by FERC, regulation by the Security and Exchange Commission, and rate, financial and organizational regulation by the state.

The Energy Policy Act of 1992 (EPACT) amended the FPA and further expanded competition within the wholesale market by allowing exempt wholesale generators (EWGs), which, once they

[44] The Atomic Energy Act of 1946 (60 Stat. 755) established the Atomic Energy Commission (AEC) to administer the transfer of nuclear power development from the military to the civilian government. The 1946 Act was changed substantially by the Act of 1954. In 1974, Congress abolished the AEC and replaced it with two agencies: the NRC, which is responsible for safety and licensing, and the Energy Research and Development Administration (ERDA), which was responsible for promotion and development of nuclear power. ERDA was later absorbed by the U.S. Department of Energy (DOE).

are so-designated by FERC approval, are exempt from PUHCA's corporate and geographic restrictions.[45] Unlike QFs, EWGs' rates or charges are unregulated. EPACT also mandated FERC to open up the national electricity transmission system to all wholesale suppliers on a case-by-case basis, thus allowing QFs, EWGs, and others to transmit their power over other utilities' transmission lines to wholesale customers.[46] This mandate significantly affected FERC's jurisdiction regarding wholesale electricity.

The recently issued FERC Orders 888 and 889 have been instrumental in achieving the goals mandated by the EPACT. Order 888 addresses the issues of open access (opening the transmission system to new generating entities) and stranded costs (recovering embedded costs of facilities that may no longer provide the specified rate of return). Order 889 mandates the formation of utility-owned information systems and requires them to publish information on the available transmission capability of all utility-owned and operated primary transmission lines (Open-Access Same-time Information System [OASIS]).

The electric industry is changing from a fully regulated, vertically-integrated structure to a competitive structure via unbundling of services and disaggregation of functions. These changes may create uncertainty as to who is responsible for reliability of the power system. Mergers and divestitures will occur as companies adjust to enter the competitive markets. Generation will be separated from transmission and marketing functions. State legislatures are grappling with new legislation to guide restructuring of the intrastate, retail electric industry. Most of the debate, however, focuses on the economic impacts of such deregulation on the local utilities, particularly the recovery of stranded costs, rather than on system reliability.

California was the first to enact a plan for restructuring. California's plan provides for recovery of stranded costs through "competition transition" charges: a current customer surcharge, and a severance fee for customers leaving the utility system to seek competitive rates elsewhere. Rates for residential and small commercial customers will be reduced beginning January 1998. This reduction will be funded by revenue bonds to finance the competition transition charges over a ten-year period. Thus California utilities should enter the competitive market without undue financial burdens.

The California plan also established an independent system operator (ISO), as recommended in FERC Order 888, to operate the transmission grid, thus eliminating preferential treatment by transmission line owners along grid corridors. The plan addresses reliability through the ISO. The ISO is to seek FERC authorization to perform its system functions and to secure the generation and transmission resources needed to achieve specified planning and operational reserve criteria. It must have standards no less stringent than those of the Western SystemsCoordinating Council (WSCC) and the NERC. It may develop inspection, maintenance, repair and replacement standards for transmission and distribution systems, specifically aimed at

[45] Both QFs and EWGs, however, are only power producers and do not own transmission facilities.

[46] The law specifically prohibits FERC from ordering wheeling of the power to a final customer (retail).

preventing system outages. The ISO, in consultation with the California Public Utilities Commission, the California Energy Commission, and other Western state agencies, would have the power to conduct a reliability study of the California interconnected transmission and generation system. The National Association of Regulatory Utility Commissioners (NARUC) adopted principles at its 1996 Summer Meeting asking legislatures to ensure reliability is maintained in the restructured industry.

As the changes resulting from these legislative and regulatory actions work their way through the industry, NERC has also had to change its focus. NERC has revised the composition of the Board of Trustees and its committees to include two new seats representing the "customer" sector. One of the new seats will likely include an industrial customer representative. The other seat has not yet been defined. This modification to the Board composition improves the representation of customer concerns. NERC also decided to sponsor an independent organization to review its present managerial and technical structure. The "Future Role of NERC" Task Force will provide its findings to the review team and oversee the review program. Recommendations are expected to be made available to the board in January 1998.

On January 6, 1997, the NERC Board of Trustees unanimously voted to obligate Regional and Affiliate Councils and their members to promote, support, and comply with all NERC reliability policies. This recent change in position from voluntary to obligatory compliance places NERC in a central position with respect to establishing national standards for system reliability.

The NERC Reliability Compliance Task Force and Future Role of NERC Task Force-II have issued a report[47] about options to ensure compliance with NERC and Regional Council policies. The report recommends that each NERC member organization establish formal coordination agreements with other relevant NERC member(s). Such agreements are to (1) specifically state the intent of the organization and its members to comply with NERC and NERC member reliability criteria and (2) establish authority to impose sanctions to ensure compliance with mandatory protocols. These agreements will then be filed with NERC. In addition, all entities performing primary reliability functions of generation control (control areas) and system security coordination must be members of the Regional Reliability Councils in which they carry out their business. To ensure membership and compliance, the report suggests that regulatory authorities require mandatory compliance with NERC reliability protocols (NERC certification) as a condition for approval of tariffs, contracts, licenses, and other instruments. The report also proposes that FERC ensure that all expenses incurred to meet reliability criteria established by NERC are fully recoverable through rates.

The NERC task force report also recommends the formation of regional security coordinators that will be equipped to evaluate regional security plans, perform transmission system assessments, and start control actions if and when reliability is jeopardized. NERC concludes that the traditional voluntary compliance approach, with the obligation and cost of providing a

[47] *Options to Ensure Compliance with NERC and Regional Reliability Council Policies, Standards and Criteria*, October 12, 1996, NERC, Princeton, New Jersey.

reliability safety net imposed on utilities entering the competitive environment, will no longer serve the needs of the new, restructured industry. The U.S. Department of Energy (DOE) Task Force on Electric System Reliability, which is to provide advice, information, and recommendations to the Secretary of Energy Advisory Board on issues related to the reliability of bulk electricity systems in the United States, has completed a draft report entitled *An Organizational Framework for Bulk Electric System Reliability: Functions and Interrelationships* (May 1997). It basically reiterates the NERC mandatory compliance suggestions.

4.2 Description of Selected Regulatory Agencies.

4.2.1 Selection Method

The following regulatory and nonregulatory agencies were selected because they represent the significant entities involved in electric utility regulation: FERC, NRC, DOE, Illinois Commerce Commission, the City of Chicago, and NERC. FERC is the primary federal regulatory body overseeing interstate wholesale electricity transactions. The NRC was chosen because it has sole jurisdiction over matters of nuclear safety at nuclear power generating stations, which account for approximately 20% of the electricity generated in the nation. The Illinois Commerce Commission was selected as an example of a state PUC in a state with a well-developed generating and transmission infrastructure. The City of Chicago was chosen as an example of local safety or reliability requirements for electric utilities operating within city limits. NERC, although not a regulatory agency, was chosen because of its historical role in assuring reliable power system operation and its current influence over the continued reliable operation of the electrical infrastructure.

4.2.2 Agency Descriptions

4.2.2.1 Federal Energy Regulatory Commission

FERC is an independent regulatory commission within DOE. Under the FPA, FERC has jurisdiction over interstate, wholesale sales of electricity by privately owned utilities.[48] FERC has the power to conduct formal and informal investigations (18 CFR Part 2). FERC is authorized to issue permits for the construction, operation, and maintenance of powerhouses, transmission lines, or other works for the development and utilization of power. It is also authorized to establish, review, and enforce rates and charges and prescribe a uniform accounting

[48] The line between federal and state jurisdiction is not always easy to determine, but the federal government's jurisdiction over electric utilities has been interpreted broadly by the courts. In *FPC v. Florida Power & Light Co,* (404 U.S. 453 [1972]), the Supreme Court found that a Florida utility's sales to another Florida utility through interconnection transmission lines, together with the simultaneous transfer of electric power from the second Florida utility to a Georgia utility, was an interstate sale within the jurisdiction of the FPC (FERC's predecessor). Thus, only clearly intrastate transmission of electricity remains under state jurisdiction (i.e., the local distribution).

system for the transmission or sale of electric energy. Therefore, every power company transmitting power in interstate commerce must file with FERC for new construction or modification of its power generation facilities and the construction of any interstate transmission lines. They must also file their rates and charges for FERC review. FERC also has jurisdiction over corporate restructuring of electric utilities, including mergers and divestitures, and has the power to order an electric utility to provide transmission services once a good faith request has been made by another utility. In addition to reviewing and approving individual projects and rates, FERC also implements policy by issuing general orders that are applicable to all regulated power companies. DOE can suggest areas for rulemaking to FERC, however, FERC is not required to adopt DOE-suggested rules or policies.

FERC also holds hearings and resolves requests for emergency interconnections made to the DOE under Section 202(c) of the FPA. FERC has specific regulations pertaining to operations during a national emergency, including moving its offices and delegating emergency powers to its staff (18 CFR Part 376). FERC regulations also provide specific exemptions from certification for certain auxiliary installations constructed solely for use during a national emergency (18 CFR 2.60).

FERC has the power to maintain and investigate compliance with its permits, and may revoke a license for non-compliance. After notice and hearing, it may levy civil penalties of $10,000 per day for non-compliance. An order for civil penalties is enforceable in any appropriate district court of the United States.

4.2.2.2 Nuclear Regulatory Commission

The Atomic Energy Act of 1954 (42 U.S.C.A. §§ 2011-2296) authorizes the NRC to regulate construction and operation of nuclear power plants. The NRC promulgates regulations, issues construction and operation licenses, maintains on-site inspection teams, and issues enforcement actions when its regulations or license conditions are violated. The NRC's jurisdiction is limited to the safety aspects of nuclear power and does not address economic regulation. In *Pacific Gas & Electric Co. v. State Energy Resources Conservation & Development Commission* (461 U.S. 190 [1983]), the Court found that the NRC regulatory scheme occupied the entire field of nuclear safety concerns, except the limited powers expressly ceded to the states, and therefore states did not have jurisdiction over the safety aspects of nuclear power plants. Conversely, the only economic considerations by the NRC are those that would affect the ability of the utility applicant to meet safety and health requirements. Therefore, all safety, construction, and operation regulations applicable to nuclear power plants are under the jurisdiction of the NRC. Because of the severe health risk and significant economic loss that could result from nuclear power plant incidents, the NRC has promulgated unusually detailed and comprehensive regulations applicable to the construction and operation of commercial nuclear power plants.

4.2.2.3 Illinois Commerce Commission

Under the Public Utilities Act and the Electric Supplier Act (220 ILCS 5/1-101 *et seq.* and 220

ILCS 30/1 *et seq.*), the Illinois Commerce Commission (Commission or ICC) has authority to supervise the generation, transmission, and distribution of electricity in the State of Illinois, including construction permitting, rate setting, and reliability standards. In general, the ICC regulatory supervision of electric public utilities is the same as that for other types of public utilities; see the detailed discussion of ICC powers and authority in Section 3.2.2.4. Generally, the ICC's focus is the economic regulation of the power industry in Illinois; however, it has issued general standards of service for electric utilities (83 IAC 410) and more specific construction standards for electric power lines (83 IAC 305).

The ICC has a general reliability policy (83 IAC 410.410 - 410.490). Under the policy each utility must provide reliable service and strive to prevent interruption of electric service. When interruptions occur, the utility must restore electric service within the shortest reasonable time. Utilities must maintain records of service interruptions, including the time, duration, and cause of each interruption. The Commission has the power to adopt electric service reliability standards.

4.2.2.4 City of Chicago

Under the Electric Supplier Act, a public utility supplying electricity within an incorporated municipality is not subject to the ICC requirements for establishing service territories and supplying service to other utility service territories. Usually, the utility operates under a franchise with the city that gives it exclusive rights to serve the city's citizens and to use the city's rights-of-way to extend and construct its facilities and lines. Commonwealth Edison has a 29-year franchise with the City of Chicago, effective until the year 2021. Commonwealth Edison is still subject to the jurisdiction of the ICC for reliability, construction permitting, and rate setting.

The City of Chicago has no specific safety or security requirements for the electric lines Commonwealth Edison maintains or constructs within the city limits. The City of Chicago Municipal Code sets out very specific requirements for building wiring, meter installation, and in-building voltage with regard to protecting the public health and safety. The City's Department of Environment, Energy Management Division, supervises Commonwealth Edison's construction and repair activities to ensure they comply with the National Electric Code, as required by the ICC.

4.2.2.5 North American Electric Reliability Council

The members of the 10 coordinated NERC Regional Councils and the one Affiliate Council represent all segments of the electricity supply industry, including investor-owned, federal, and rural electric cooperatives; state/municipal and provincial utilities; independent power producers; and power marketers. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. Members from these entities provide unmatched expertise in the planning, engineering, and operating aspects of electric system reliability for NERC's Engineering and Operating Committees. These committees

and their subgroups serve the collective needs of the industry by researching and resolving North American operational and planning issues.

NERC members have historically volunteered to comply with established NERC policies, procedures, principles, and guides to ensure a reliable power system.[49] More details on specific operating policies and NERC's move toward obligatory compliance follow in the next section.

4.3 Regulations and Critical Infrastructure Protection

4.3.1 Impact of Regulations on Critical Infrastructure Protection

System Vulnerabilities and Threat Scenarios

The loss of a power system component (generator, substation, or other piece of equipment) threatens the generation capacity available to serve the loads attached to the transmission network. If sufficient generation and transmission reserve margins are available, system disturbances may be minor and sags may not be noticeable, because other online system components respond to the system changes. Continued system operation under these conditions relies on adequate generation and transmission capacity within and between the areas surrounding the affected component. In more extreme cases, inadequate generation and/or transmission capacity can cause electricity from the main power system to be cut off (or shed load). Isolated islands may form that are left either without a power source or with a power source that is extremely vulnerable to additional problems. This situation could affect a large number of customers connected to the isolated transmission system and reflects an undesirable system emergency state that calls for careful system restoration procedures.

The following scenarios describe possible threats to or system conditions of the electrical infrastructure. Some situations describe a general concept that characterizes a particular operating phenomenon. Other situations highlight the potential for direct sabotage. For all situations, possible remedies to alleviate these conditions or threats or practical ways to improve current methods of evaluation are discussed. The discussion also addresses contingency planning, which can mitigate the impact of sabotage on the reliability of the infrastructure if preventive measures prove inadequate.

An operating failure can result from either natural causes or deliberate means. The utility's response, however, is independent of how the component is taken out of service. As a result, a system designed to operate under a given set of system disruption contingencies will remain operable and reliable. Contingencies represent a transmission line, generating facility, or some other piece of equipment that is taken out of service (becomes inoperable) because of a natural disaster (e.g., lightning), equipment failure, or malicious act.

---

[49] *Policies, Procedures, and Principles and Guides for Planning Reliable Bulk Electric Systems*, June 1995, and *NERC Operating Manual*, December 1996, NERC, Princeton, New Jersey.

In most respects, isolated sabotage events (single instances of deliberate attack) can be regarded as single contingency events. These are usually addressed in utility/system contingency planning. On the other hand, coordinated sabotage events representing multiple contingencies are very difficult to predict and therefore may not always be adequately addressed in developing a system contingency list to be considered for emergency planning. The effects of multiple sabotage events pose the greatest threat to the electrical infrastructure.

Physical Threat

The loss of a power plant can be accomplished in several ways. Access to plant surroundings provides a way to modify fuel supplies or disable primary transformers, generating equipment, or system controls. Each scenario results in a different degree of plant malfunction; for example, altering the fuel supply has less severe results than bombing the turbine-generator. However, the same system effect is achieved — the plant's generation capacity is removed from service. Risk of this type of occurrence could be reduced through use of fencing, closed-circuit TV, or security forces, although these measures would involve costs.

Most substations are unmanned and therefore face an increased risk of sabotage. Like most substations, transmission lines are located in remote areas, and a person may have air or ground access to utility rights-of-way with little or no chance of being spotted. In addition, transmission towers can be felled. It should be noted, however, that they are built to specifications designed to ensure survival in violent weather. Some instances of attempted sabotage were unsuccessful because detachment of one or even two legs of a four-legged tower did not bring it down.

An easier way of removing a line from service is to shoot the insulators suspending one of the transmission conductors. The result is a short circuit when the line comes in contact with the ground.

Cyber Threat

Cyber threats to control systems are also a concern. Sophisticated electronic systems are used in operating large electric utility generation and transmission facilities. These systems rely on large databases, remote sensoring, and telecommunications between NERC members to maintain control of the energy flow and to ensure system balance. Malicious action against system components controlled by Supervisory Control and Data Acquisition (SCADA) is possible. Hackers could, for example, record control signals that were sent over conventional communications channels and play them back later, causing unscheduled system interference. Research and development activity to address this problem was recently a topic at the Institute of Electrical and Electronics Engineers (IEEE) 1997 Winter Power Engineering Society Meeting ("Information Security Issues in Utilities"). Encryption methods are available; however, utilities would have to upgrade older equipment to accept the additional protocol.

Regulatory Security Requirements for Nuclear Power Plants

All commercial nuclear power plants must obtain a license from the NRC. NRC regulations specifically state an applicant is not required to provide for design features or other measures for the specific purpose of protection against attacks, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person (10 CFR 50.34). However, the regulations provide for design criteria and performance standards for protection against radiological sabotage. Under NRC regulations (10 CFR 73.1(a)(1)), the definition of radiological sabotage includes deliberate acts directed against a nuclear power generating station that could endanger the public health and safety by exposure to radiation. In establishing physical security requirements, the NRC defines radiological sabotage as (1) a determined violent external assault, attack by stealth, or deceptive actions of several persons who are dedicated and well-trained (including military training and skills), (2) possibly using inside information or assistance, (3) possessing suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and long-range accuracy, (4) possessing hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity, and (5) using a four-wheel-drive land vehicle used for transporting personnel and their equipment. It can also include an internal threat of an insider, including an employee and a four-wheel-drive land vehicle bomb. A successful act of nuclear power plant sabotage would likely cause significant damage to the plant and possible permanent shutdown. There would also probably be a significant temporary or permanent loss of electrical generating capacity and economic loss to the operating utility.[50]

The NRC regulations cover design criteria that specifically address security (e.g., built-in redundancy, physical separation of independent circuits to minimize the likelihood of simultaneous failure, and control and monitoring equipment necessary to maintain a radiologically safe condition during emergencies [10 CFR 50, Appendix A]). These design features must ensure that the plant is able to withstand and recover from a station blackout and be capable of shutting down the reactor and maintaining it in a safe condition. In addition, each application for a permit must include a physical security plan that addresses the identification of vital equipment, vital areas, and the security systems and subsystems designed to protect them. It must also include a safeguards contingency plan for dealing with threats, thefts, and radiological sabotage in conformance with the requirements found in NRC regulations for physical protection for plants and materials (10 CFR 73).

NRC regulations for the physical protection for plants and materials require the capability to prevent entry of unauthorized persons, vehicles, and materials into material access areas and vital areas. This capability must include a (1) physical barrier system for all vital areas, such that

[50] NRC regulations also contain detailed specifications for emergency response capabilities on the part of nuclear utilities and nearby communities; these are discussed in Section 9.

access to them would require passage through at least three barriers, and (2) perimeter protected by two separate physical barriers, with an intrusion detection system between the two. The barrier must incorporate features to prevent forcible vehicle entry. Isolation zones must be maintained adjacent to all outdoor physical barriers to allow observation of all persons or activities on either side of the barrier. The protection system must be able to detect any attempts to gain unauthorized access or to introduce unauthorized material across the plant boundary by stealth or force. Access to vital areas is limited to those employees whose duties require them to enter the area.

The plant must have an established, trained, and qualified security organization that can execute planned responses to emergency and safeguard contingency events (tactical response team). The regulations recognize internal and external threats. For instance, no plant can assign a member of the security organization to have direct operational control over more than one of the redundant elements of a physical protection subsystem if it could result in loss of effectiveness of security performance. All security personnel must meet stringent performance standards concerning physical health and weapon proficiency and undergo an FBI criminal history investigation.

These physical protection systems must be maintained and tested periodically; tests must include real-time exercises. The plant cannot make changes to its safeguards contingency plan that would decrease the effectiveness of the security plan or guard training and qualification plan without prior approval of the NRC. Therefore, sabotage against a nuclear plant would require an extremely well-trained, well-equipped terrorist force or the criminal intent of a very high-placed, knowledgeable employee. Other components of the power system are not so well-protected.

Regulatory Security Requirements for Nonnuclear Facilities

Policy 4 of the *NERC Operating Manual* requires only minimal physical security for electric systems. This policy requires monitoring equipment that will bring important deviations in operating conditions to the system operator's attention and will indicate, if appropriate, the need for corrective action. Each control area must have sufficient metering to ensure accurate and timely monitoring of operating conditions under both normal and emergency situations, including evaluating the loss of significant transmission or generation facilities. Policy 4 also provides that, where practical, critical unmanned facilities should be monitored for physical security, and, at a minimum, scheduled inspections and preventive maintenance should allow the utility personnel to monitor the conditions of these facilities.

The Illinois Commerce Commission regulations do not require specific physical security for any component of an electric utility's system. They do provide that all electric supply and communication lines and equipment must (1) be defined, constructed, and maintained to meet those portions of the National Electric Safety Code adopted in the regulations (83 IAC 305) and (2) generally be able to provide safe, adequate, and dependable service. All distribution lines must have protective devices to effect shutdown in case of a power surge.

Ensuring Reliability after an Interruption

No federal or state regulatory body or legislation provides a concise definition of reliability; therefore, it is appropriate to adopt the definitions and standards of NERC as the basis for discussion. NERC defines *reliability* as the "degree to which the performance of the elements of that system results in power being delivered to customers within accepted standards and in the amount desired."[51] A reliable power system gives customers what they want, when they want it. The "ability of the bulk power electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components" refers to the *security* of the power system. There is a relationship between reliability and system security in that a secure system assures a reliable system. A secure system remains operable after system emergency contingencies occur; it also successfully adjusts for transmission or generating capacity that was removed because of the loss of a critical component. A reliable system provides the adequacy and security needed to react to emergency contingencies. The ability of a system to adjust and continue service after loss of a critical component is what ensures the viability of the electric infrastructure when preventive measures have failed.

The NERC regions all practice methods to measure and model system security.[52] Models are created to simulate the system impacts of individual and multiple contingencies. A single contingency represents a single component failure. Considering the size of a power system, there are literally millions of possible contingencies. Model simulations are used to understand the system response to these contingencies and to assure continued system operation. Operational guidelines that direct how system operators are to adjust the system if such events take place result from these simulations. The practice of modeling these system contingencies greatly contributes to the reliability of the electric power infrastructure.

A critical element of these studies is the accuracy of the selected contingencies. A great deal of system expertise, effort, and advanced modeling software is expended in defining the contingencies represented on the contingency list. If a specific contingency is not explicitly modeled, the system response to it cannot be examined and anticipated. The NERC Reliability Assessment Subcommittee (RAS) reviews and assesses the overall reliability of the regional bulk electric systems to ensure that each Region conforms to its own planning criteria. The planning reliability criteria of the Regional Reliability Councils are published by the Reliability Criteria Subcommittee (RCS). Thus the RCS would be a logical group to consult regarding inclusion of sabotage-based scenarios in contingency planning.

In situations of direct sabotage, a piece of equipment is "prematurely" taken out of service. Regardless of whether a component naturally fails or is deliberately made to fail, the event is viewed as a single contingency that may be represented in the contingency list. This concept is important to understand, since standard modeling practices apply equally to deliberate events and

[51] *Reliability Concepts*, NERC, Princeton, New Jersey, February 1985.

[52] *Overview of Planning Reliability Criteria of the Regional Reliability Councils of NERC*, North American Electric Reliability Council, Princeton, New Jersey, April 1988.

natural events. As long as the contingency is a member of the contingency list, the event can be simulated, system security can be evaluated, and impact mitigation can be planned. In a similar manner, selected multiple contingencies are included in the contingency list, although they pose a greater threat to continued system security. This information must be kept in mind when considering the impact of deliberate power system attacks.

The steps involved in selecting, simulating, and evaluating the impacts of contingencies is considered a system planning activity. In the event that contingencies do occur, NERC policies dictate how the industry is to respond to these events and report them. An example of these policies are found in the *NERC Operating Manual*. It presents specific criteria, requirements, and guidelines with regard to particular system operating characteristics and procedures. Guidance is provided for generation control, transmission, system coordination, emergency operations, operations planning, telecommunications, and operator training issues.

The *NERC Operating Manual* addresses the need for each utility in the control area to maintain a level of operating reserve sufficient to account for system equipment forced outage rates. Following loss of resources or load, a control area must take appropriate steps to return the system load to its predisturbance level within 10 minutes after the start of the disturbance. When an operating emergency occurs, a prime consideration is to maintain parallel operation throughout the interconnection. Each system and control area must promptly take appropriate action to relieve abnormal conditions. A system, control area, or power pool that experiences or anticipates an operating emergency must communicate its current and future status to neighboring systems throughout the interconnection. Systems able to provide emergency assistance then make their capabilities known to the burdened system. Other systems may be notified through predetermined communication paths whenever the system suspects or has identified a multi-site sabotage occurrence or a single-site sabotage of a critical facility. If necessary, the system has a predetermined methodology for shedding load to accommodate the entire interconnected system.

An issue recently arose concerning the original NERC System Coordinators Committee proposal for prioritizing customers, which allowed a utility to interrupt nonutility firm customers before utility firm customers. The proposal was in contravention of FERC's *pro forma* tariff regulations, which prohibit discrimination between similarly situated customers (i.e., all firm customers). NERC and FERC worked together informally to redraft the proposal to meet FERC nondiscrimination requirements, using a *pro rata* interruption methodology for all similarly situated customers whose load was determined to be affected by the contingency.

All disturbances or unusual occurrences suspected or determined to be caused by sabotage must be reported to the appropriate governmental agencies, including the FBI and regulatory bodies. Each control area must have procedures for recognizing sabotage events on its facilities and multi-site sabotage affecting larger portions of the interconnection and for making its system operators aware of them.

A set of plans must be developed and implemented for each system, control area, pool, and region within NERC to cope with operating emergencies. These plans must enable the system or

pool to mitigate, to the fullest extent possible, the effect of a capacity or energy emergency on its customers. These must include operating and coordinating agreements between neighboring systems or pools to provide emergency assistance. Such assistance may include supplying reserve generating capacity for a limited period of time. The system operators also must have authority to implement manual load shedding when necessary.

Reports of any emergency conditions or abnormal events, which in the opinion of the reporting utility could constitute a hazard to maintaining the continuity of the bulk electric power supply system, must be reported to the DOE Emergency Operating Center (EOC) within 24 hours. The *NERC Operating Manual* provides for regional and interregional emergency telecommunications networks in Appendix 7A. Each network consists of a preset conference call that interconnects coordination centers in the regions within each interconnection. The *NERC Operating Manual* even sets out call procedures. There are hotlines for aid in emergency or near-emergency situations, which cannot be solved by normal contiguous interconnected system communications. The telecommunication networks are to be tested weekly to assure operation during emergency conditions.

NERC consistently modifies and updates these policies as specific events reveal policy deficiencies. Considerable practical experience has been gained from analyzing actual system disturbances.[53] These studies provide insight on whether to reenforce or change existing policies. Most of these events represent localized problems that affect a small number of customers, if any. In the event of a large-scale incident, NERC assigns focused task forces to study and publish a detailed accounting of the events leading up to the specific situation.[54] Both report formats typically summarize the situation, describe the sequence of events, describe power restoration procedures, draw a series of conclusions, and identify a set of recommendations intended to prevent similar incidents. Similarly, specific changes to NERC policies may be proposed to reduce the likelihood of reproducing similar situations in the future. Again, NERC's methods provide a proactive means of acquiring and including lessons learned into operational procedures to increase overall system reliability.

Availability of Sensitive Data

FERC Form 715, *Annual Transmission Planning and Evaluation Report*, provides NERC regional load flow data to the general public. This data could be used by an experienced energy system modeler to pinpoint potential weak network facilities or interconnections. This poses a risk to system security by providing information on the system topology and likely vulnerable areas. Unrestricted access to this data was a controversial issue before Form 715 was ordered. Now the FERC bulletin board system (BBS) offers the data free of charge. Anyone can log onto the BBS by typing a name and password; there is no mechanism to verify the name or company

[53] *System Disturbances*, NERC, Princeton, New Jersey, July 1996.

[54] For example, see *Report on Electric Utilities' Response to the Cold Wave of January 1994*, NERC, Princeton, New Jersey, April 1994.

affiliation. The system provides downloadable data files, including annual reports, rates, planning area reports, and other documents. In addition, similar information, including the date, time, duration and cause of outages experienced by every NERC member, is available on the NERC Internet site (http://www.nerc.com/dawg/database/dawg-96.html). The exact potential for abuse is difficult to determine, since some amount of system expertise is still required to derive a contingency set that causes trouble. However, it is possible that access to this data could enable an intelligent hostile element to establish a contingency list, prioritize the effects of represented contingencies, and produce a multiple contingency disturbance that could bring down the system in some manner. Access to the contingency set, whether derived from the FERC Form 715 data or purchased from a disgruntled utility employee, poses a significant risk to electrical infrastructure protection.

In addition, with the development of the OASIS, even more information will be easily available concerning the routing of interstate, wholesale electric sales throughout the nation. Also, to facilitate the wheeling ordered by FERC Order 888, independent system operators (ISOs) (centralized control points) may be developed for many power pools and interconnections to broker the movement of electricity from control area to control area.[55] This again will tend to concentrate information on generation and transmission adequacy in one database.

4.3.2 Measures for Improvement

From discussions and professional interactions at conferences and meetings, one can sense that utilities sincerely want to provide a reliable product to their customers. As it does in any business, risk plays a role in both reliability and earnings. If utilities had the option, they would install state-of-the-art equipment designed to provide the most reliable operation for their given transmission and distribution network configuration. However, in the deregulation climate it is necessary to closely monitor costs. The open market will send the proper price signals when transmission bottlenecks become a limiting factor in assuring economical power.

One simple improvement in the present regulatory structure would be to reduce the red tape associated with recovery of costs incurred to improve reliability. The NERC report, *Options to Ensure Compliance with NERC and Regional Reliability Council Policies, Standards and Criteria*, recommends that FERC ensure that all expenses incurred to meet reliability criteria established by the NERC are fully recoverable through rates. After short-run improvement costs are recovered, the long-run benefits of relieving these bottlenecks are as follows: increased transfer capability, increased transmission margins, improved operating flexibility in the event of natural or deliberate interruptions, and reduced customer costs.

[55] In the California electric utility restructuring scheme, when the ISOs are formed the utilities will transfer their transmission grids to the ISO and either sell or lease their control centers (computers and all) to the ISO.

The analysis of regulatory impacts on critical electrical infrastructure protection in Section 4.1 suggests four areas for possible initiatives to improve security. Three of the four are aimed at preventing attack, and the fourth is aimed at preventing widespread consequences from an attack.

1. *Develop higher standards for physical security at vulnerable nonnuclear facilities.* As discussed, security standards for nuclear power plants are extensive and apparently effective. Security standards for physical protection of nonnuclear facilities such as power plants and substations are much narrower in scope. To improve overall system security, one approach would be to research cost-effective measures to enhance security at such facilities. A model standard for implementing such measures could then be developed for adoption by NERC and state regulatory bodies. Uniform application of requirements would help ensure that these measures do not interfere with the market by favoring some firms over others.

2. *Develop methods for protecting against cyber attack on control systems.* As discussed, network control systems are considered vulnerable to intercept and interference. An obvious response would be to develop methods or protocols for protecting this information, either through the use of physically secured transmissions or through encryption or other data-protection methods. Regulatory action to require use of such protections may be appropriate since they might be cost-effective from an overall system standpoint, yet not so from the standpoint of any given company.

3. *Control key information that identifies system vulnerabilities*. Information on system configurations that might benefit hostile elements is currently available over the FERC BBS, on the Internet, and via Freedom of Information Act requests. Placing controls on such information might serve a protective function. However, research would be needed to determine whether (1) information can practically be controlled without substantially interfering with normal or emergency operations and (2) control of this information would run counter to any current regulatory disclosure requirements.

4. *Add more sabotage-based scenarios to NERC contingency modeling and planning.* Modeling and planning for system contingencies by NERC is the main method by which the electric industry assures that local emergencies do not become regional or national emergencies. Some sabotage-based scenarios are already part of this planning. It might be worthwhile for a government-industry group to examine this planning and determine whether other plausible scenarios should be considered.

5 OIL AND NATURAL GAS INFRASTRUCTURE

5.1 General Description of Regulation

5.1.1 Current Regulatory Environment

Natural Gas Industry Profile

Natural gas is produced at privately owned wells located throughout the United States. Some wells are located on private lands. Others are located on federal lands leased from the U.S. Bureau of Land Management (BLM) or under leases of rights on the Outer Continental Shelf (OCS), which is under the jurisdiction of the U.S. Department of Interior (DOI), Minerals Management Service (MMS).[56] The gas is pumped, either as a by-product of oil production or as a singular product, and transported along gathering lines to a consolidation/compression facility. Natural gas is also imported from (and exported to) Canada and Mexico along international pipelines. Liquefied natural gas (LNG) is also imported via tank ships to port facilities where it is stored, then converted to the gaseous form for pipeline shipment. The safety regulation of LNG facilities is under U.S. Department of Transportation (DOT) jurisdiction. However, states may have requirements for liquefied petroleum gas (LPG) and compressed natural gas (CNG) facilities.

The gas is then transported along a network of interstate and intrastate pipelines that traverse the 48 contiguous states and Alaska. These pipelines are owned and operated by pipeline companies. Pipeline companies are engaged in the transportation of natural gas; however, these companies may have sister divisions or companies engaged in production or distribution operations. The gas can be delivered to the ultimate consumer either directly from the pipeline, as is the case with some industrial or commercial facilities, or to an interconnection (city gate) with a local distribution company (LDC) for transportation along distribution lines to homes and businesses.

Overview of Natural Gas Regulation

As discussed below, each of the natural gas system components (production, transportation, and distribution) is regulated by different regulatory bodies.

[56] MMS has jurisdiction over areas except those specific areas under state jurisdiction that are delineated by using a formula. For Texas and the Gulf Coast of Florida, it is three marine leagues (approximately nine nautical miles) seaward from the baseline from which the breadth of the territorial seas is measured.

- Production facilities are subject to both economic and environmental regulation. Economic regulation of natural gas production addresses well drilling, well management, and management for gathering, treating, and compressing gas for pipeline transmission. In general, privately owned production facilities are under the jurisdiction of the state in which the facility is located. Production facilities located on federal lands are regulated via the terms of their lease by the BLM. The MMS exercises control via lease terms of facilities located on the OCS. Production-related facilities are also subject to environmental regulation by the U.S. Environmental Protection Agency (EPA) and its authorized state counterparts. Applicable environmental regulations include those pertaining to waste disposal and air emissions.

- For interstate pipelines, the economic aspects of wholesale transportation and sales of natural gas are within the jurisdiction of the Federal Energy Regulatory Commission (FERC). Pipeline safety and construction standards for interstate transportation pipelines are under the DOT.

- For intrastate pipelines and LDC distribution lines, pipeline safety and construction standards are within the jurisdiction of the state agency (certified by DOT). The economic aspects of intrastate, retail transportation and sales of natural gas (intrastate pipeline companies and LDC public utilities) are regulated by the state public utility commission (PUC).

Oil Industry Profile

Like natural gas, oil is produced at privately owned facilities located throughout the United States. These facilities may be located on private land or on leased federal lands, including the OCS. Although there are small independent producers, the major oil companies (the 20 largest, vertically integrated, multinational oil companies) predominate the oil industry. The independents vary in size and generally are not involved in every stage of the oil industry. Most engage only in production and sell their crude product to the major oil companies or to smaller independent refineries. In the case of gasoline, the oil companies and refiners sell to other wholesalers or sell at retail from their own gas stations or under contract with independent gas stations. Other grades of oil are also sold to end users or to retailers (e.g., fuel oil suppliers). In some cases, oil or oil products are shipped via pipeline directly to large industrial customers. Most wholesale transportation is by pipeline or truck to a local end terminal, where the product is stored and then transported by truck to individual customers such as gasoline stations.

Overview of Oil Regulation

The regulation of oil production facilities (including treatment facilities such as refineries) is generally under state jurisdiction, except for facilities operating under lease on federal lands or the OCS. Oil producers are generally subject to state regulations concerning well drilling, well management (including maximum production limits), gathering equipment, storage, and refining.

They are also subject to environmental regulations (including requirements for spill prevention and emergency response) administered by the EPA and its authorized state counterparts. Emergency response and personnel safety for off-shore production facilities on the OCS come under the jurisdiction of the U.S. Coast Guard and MMS. However, pipelines running from production facilities to on-shore facilities (that are not gathering lines) are under the jurisdiction of DOT.

Safety and construction standards for interstate oil transportation pipelines are under the jurisdiction of DOT. Intrastate pipelines are similarly regulated by state agencies under DOT-certified programs. Most economic regulation of oil pipeline construction, both interstate and intrastate, ended in 1994. However, oil pipelines must still file simplified rates and tariffs for transportation services with the FERC (18 CFR Parts 340-342).

Complexity of the Oil and Gas Regulatory Scheme

The regulatory scheme for oil and gas is complex and divided among many agencies. There are numerous provisions and exceptions to particular parts of the scheme for particular types of equipment or situations. In some cases, the scope of a particular agency's jurisdiction may extend only to production equipment or only to transmission or distribution equipment, but the real world of oil and gas systems does not always fall neatly into these categories. Therefore, determining who has jurisdiction and what rules apply to a given location is sometimes difficult. For example, DOT has issued regulations prescribing minimum safety standards for pipeline facilities, covering the construction, maintenance, and operation of gas and oil interstate pipelines. The scope of these regulations includes the gathering, transmission, and distribution of gas by pipeline and the storage of gas, but does not include the gathering of gas through unregulated gathering lines in rural locations located outside the limits of any (1) incorporated or unincorporated city, town, or village; (2) any other designated residential or commercial area (including a subdivision, business, shopping center, or community development); or (3) similar populated area. DOT-regulated transportation of oil includes the movement of petroleum or petroleum products by pipeline or the incidental storage of such products but does not include oil moving through gathering lines in a rural area; on-shore production, refining, or manufacturing facilities; or storage or in-plant piping systems associated with on-shore production, refining, or manufacturing facilities. The safety aspects of gathering lines and distribution lines in rural areas or within production facilities are generally under the jurisdiction of state pipeline safety regulation.

The complexity of the regulatory scheme may or may not be a problem for the oil and gas industry *per se*; however, it can complicate efforts to institute changes in the regulations to accommodate new policies.[57]

[57] See Appendix A to 49 CFR Part 195 - Delineation Between Federal and State Jurisdiction - Statement of Agency Policy and Interpretation.

5.1.2 Current Trends in Regulation

Deregulation of Natural Gas

Federal regulation of natural gas began with the Natural Gas Act (NGA) passed in 1938. Regulation of natural gas under the NGA was implemented by the Federal Power Commission (FPC).[58] The NGA allowed pipelines to transport gas from producers to customers across state boundaries. The NGA applied to interstate pipeline companies only; gathering, production, and distribution facilities were not included. However, the FPC's jurisdiction under the NGA was extended to producers by the Supreme Court.[59] After a relatively long quiet period, oil and gas shortages in the 1970s led to a series of legislative changes. In 1978 Congress passed the Natural Gas Policy Act (NGPA), which moved from cost-based, utility-type regulation toward a pseudo-free market pricing scheme. The NGPA had a built-in time schedule for price deregulation, and a substantial portion of gas was deregulated by January 1985. In 1989, the Natural Gas Wellhead Decontrol Act (NGWDA) removed all remaining NGPA wellhead price controls and eliminated all NGA filing requirements for natural gas producers. This situation created a competitive market and the start of market-based wholesale rates. As discussed below, pursuant to FERC Orders 436 and 636, producers and users of natural gas now have open access to the network of pipelines on a contractual basis with pipeline companies. However, FERC still requires pipeline companies to obtain approval for corporate merger and divestiture, obtain permits for constructing interstate pipelines, and file rates for transporting natural gas along those pipelines and for operating storage facilities connected to the pipeline.

The 1980s brought gradual deregulation of natural gas production pricing. In 1984, FERC issued Order 380, which outlawed minimum bills, giving customers the opportunity to purchase low-cost supplies while avoiding the high-cost old contracts. The following year, FERC issued Order 436, which required pipelines to provide separate transportation service to other producers, thus allowing marketers and end-users to compete. Finally, FERC Order 636 (August 1992) completed deregulation by forcing pipelines to fully unbundle their merchant, transportation, and storage services, thereby allowing for market-based prices and creating a secondary pipeline capacity market.

The recent changes in federal regulation of natural gas pricing effectively segment the industry into three parts: producers, interstate pipeline operators, and intrastate pipelines and distribution networks. Members of each of these groups are now more or less free to contract for the sale, purchase, and transportation of natural gas on an as-needed basis and at mutually negotiated prices. However, there is still federal oversight, and the federal government can act to alleviate shortages if they occur.

---

[58] The FPC was the predecessor to the FERC. Intrastate pipelines (Hinshaw pipelines) are not subject to NGA jurisdiction but to the jurisdiction of the applicable state agency.

[59] *Interstate Natural Gas Co. v. FPC*, 331 U.S. 682 (1947) and *Phillips Petroleum Co. v. Wisconsin*, 347 U.S. 672 (1954).

At the state level, the trend is for state PUCs to follow the federal pattern of deregulating pricing. However, other aspects of state-level regulation, such as well production limits and pipeline safety requirements, are still closely regulated, as detailed below.

Deregulation of Oil

As did natural gas regulation, oil industry regulation underwent significant changes beginning in the 1970s, leading to wholesale pricing deregulation in the 1990s. The Emergency Petroleum Allocation Act of 1973 (EPAA) gave broad authority to the President to regulate oil production and wellhead prices to stimulate domestic exploration and production. The President was also authorized to establish priorities among end users in times of shortage. In 1979, President Carter used his EPAA authority to begin a phased decontrol of oil and oil products regulation. Economic regulation of oil products was essentially ended under Executive Order 12287 (January 28, 1981). In 1992, FERC jurisdiction over oil transportation pipelines was reduced to the acceptance of simplified rate filings, and in 1994 FERC's authority over permitting the siting and construction of oil pipelines was repealed altogether. Although the federal economic regulation of oil and natural gas production has in effect ended, production functions and pipeline construction are still regulated at the state level.

The deregulated oil industry is in an economically challenging situation. The number of refineries has decreased from more than 300 to 165 over the past 15 years. The profit margins have decreased while the competition, particularly from overseas companies, has increased. There has been an increase in environmental regulation, in part from the closing of loopholes and exemptions that once protected the industry. Recent environmental trends include (1) producers having to report data for the EPA's Toxic Release Inventory, (2) compliance with air quality standards, (3) an increase in safety programs, and (4) restricted exploration. All of these result in increased costs to the oil industry. The EPA's Toxic Release Inventory requirements are projected to cost producers more than $100 million per year. Increased air quality standards and reduced emissions require major capital investments in environmental technologies. In addition, because of environmental concerns, some potential oil-producing areas, such as the Arctic Refuge and recent finds off the coasts of Florida and North Carolina, are not being opened up to producers. These regulatory changes and access restrictions will ultimately increase the cost of production and lower the amount of domestic production.

In addition, the construction of new natural gas and oil pipelines must now confront the opposition of environmental groups and communities. Recently in Illinois, a request for permission to build an oil pipeline through a suburban area was denied by the Illinois Commerce Commission for failure to demonstrate a public need. The Commission found the desire of one

refinery to obtain lower-cost, additional oil supplies was not sufficient to establish a public need and invoke the Commission's power of eminent domain, when compared with the concerns of affected communities.[60]

Decreased Margins in Capacity

Economists link competitive markets and efficient markets together. The assumption is that the gas and oil suppliers will meet the demand, provided consumers are willing to pay to maintain adequate supplies. However, there may be some potential pitfalls to consider. Under pure competition, pipelines must operate at high utilization rates to keep costs down. Each pipeline will optimize its own deliveries without consideration for the network system or for establishing emergency supplies. The excess capacity on the existing pipeline infrastructure will decrease, thereby reducing the current transportation system redundancy.

Use of Risk Analysis in Setting Requirements

DOT, EPA, the Coast Guard, and state agencies still strongly regulate the safety of pipelines and production and storage facilities. The recent reauthorization of the Pipeline Safety Act (Accountable Pipelines Safety and Partnership Act of 1996) does not erode the safety standards set for pipelines. However, for the first time, it does provide for the systematic application of a risk management scheme to its rulemaking process and to the industry's implementation of the regulations. This new approach provides that safety standards prescribed by DOT must be not only practicable and designed to meet the need for gas pipeline safety but must also consider the reasonably identifiable or estimated costs and benefits expected to result from the new standard. In conducting the risk assessment, DOT must identify the regulatory and nonregulatory options considered in prescribing the new standard and the associated costs and benefits. However, this balancing is not required when the regulation is the product of negotiated rulemaking or the adoption of industry standards that receive no significant adverse comment after notice in the *Federal Register*.

To ensure continued pipeline safety, under the current rulemaking process, proposed standards are reviewed by the Technical Pipeline Safety Standards Committee and the Technical Hazardous Liquid Pipeline Safety Standards Committee. These committees are made up of individuals from the federal government, state government, natural gas or petroleum industry, and general public. They review each proposed standard and publish a committee report on its technical feasibility, reasonableness, and practicability. Although the DOT Secretary is not bound by the conclusions of the committees, if the Secretary adopts regulations in contravention to the report, the reasons for deviation must be published. In addition, the committees may propose safety standards to the Secretary for adoption.

[60] *Lakehead Pipeline Company* (Ill.C.C. Docket No. 96-0145). The applicant did not need Commission approval to construct the pipeline but required a Certificate of Good Standing in order to exercise the right of eminent domain.

Under the Accountable Pipelines Safety and Partnership Act of 1996, a risk management demonstration program is to be established, with the voluntary participation of gas and oil pipeline operators. The volunteers will submit risk management plans that contain measures designed to achieve an equivalent or greater overall level of safety (compared with DOT standards) with increased efficiency and cost-effectiveness. The expectation is that through the application of some form of risk assessment of the volunteer's systems, areas needing the greatest risk reduction will be identified. The company will have the opportunity to design and propose plans based on risk modeling that may deviate from the current standards but can be demonstrated to lead to greater levels of systemwide safety at lower cost. This program is still in the formative stage.

Increase in Liability Exposure

One other recent legal change that has affected safety practices is the increase in liability exposure provided for in the Oil Pollution Liability and Compensation Act of 1990. Specifically, the Act allows for unlimited liability for negligence or willful misconduct and increased liability for oil spills. Although not regulatory in nature, this change in the legal landscape drove upgrades in many of the transport vessels.

Proposals by Industry Associations

Although they are not regulatory bodies, the Interstate Natural Gas Association of America (INGAA), American Gas Association (AGA), and Gas Research Institute (GRI) are influential in setting national policy concerning the operation of natural gas production, transportation, distribution, and storage facilities. The INGAA and AGA closely monitor legislation and rulemakings that may affect the natural gas industry. All three associations participate in research and studies on new technologies and economic market conditions. GRI has prepared two topical reports concerning the future of gas safety issues under deregulation.[61] These reports conclude that the trend for deregulation is a positive change and "the increased use of voluntary programs that are co-designed by government and industry can result in compliance with safety goals in a more efficient manner." However, they also find that "more flexible regulation, while introducing opportunities for cost savings, also introduces less certainty, a greater need for decision-making and documentation, and a lengthy learning curve." They also postulate that the shift away from federal regulation to state regulation could result in less uniformity in safety regulation. The reports stress that the cost-cutting requirements associated with the newly competitive market may result in a smaller, untrained workforce that will not have sufficient knowledge to implement the necessary safety procedures. The reports also express concern with the new risk management demonstration program and whether it will result in a perception by the public that safety requirements are being reduced.

[61] *The Future of Gas Safety Issues: Views from Outside the Industry*, GRI-96/0198, June 1996, and *Trends, Issues and Recommendations for Natural Gas Safety: Views from the Industry*, GRI-96/0410, December 1996.

5.2 Description of Selected Regulatory Agencies

5.2.1 Selection Method

The following agencies were selected for detailed discussion: DOT, EPA, DOE, Illinois Commerce Commission (ICC), and Texas Railroad Commission (TRC). DOT establishes the basic safety standards for interstate transportation of natural gas and oil via pipeline and for the construction and operation of LNG facilities. These DOT standards are then adopted and enforced for pipelines by the states. The EPA establishes spill response requirements for petroleum and petroleum product storage facilities[62] and environmental standards for the oil production industry. DOE is included as the policy-setting body for all energy industries. The ICC was chosen as an example of a state PUC that regulates natural gas public utilities and gas pipelines. The TRC was chosen as an example of the regulation of oil and natural gas production facilities in a major oil- and natural-gas-producing state.

5.2.2 Agency Descriptions

5.2.2.1 Department of Transportation

The Pipeline Safety Act (PSA) (49 U.S.C.A. 60101 *et seq.*) authorizes DOT to establish minimum safety standards for oil and natural gas pipelines. DOT has responded by issuing standards that apply to all owners and operators of pipeline facilities. The standards address design, installation, inspection, testing, construction, extension, operation, replacement, and maintenance of pipelines and emergency plans and procedures for them. As discussed above, these standards are promulgated via a cooperative system that allows federal and state government, industry, and public participation through the Technical Pipeline Safety Standards Committee and the Technical Hazardous Liquid Pipeline Safety Standards Committee.

The DOT Office of Pipeline Safety[63] has primary enforcement jurisdiction over interstate transportation pipelines. Primary enforcement responsibility for pipelines is delegated to the states, with DOT supervision. Each state authority must submit an annual certification to DOT, showing that it (1) has regulatory jurisdiction over the pipelines; (2) has adopted regulations at least as stringent as the DOT safety standards and regulations; (3) has the legal power to enforce and is enforcing each adopted standard; and (4) is encouraging and promoting programs designed to prevent damage by demolition, excavation, tunneling, or construction activity to the pipeline facilities under its jurisdiction. In addition, the certification may show that the state requires record maintenance, reporting, and inspection programs substantially the same as those provided in the DOT regulations.

---

[62] End terminal storage facilities are under the jurisdiction of the EPA. Storage facilities incidental to the transportation of oil along oil pipelines are under the jurisdiction of DOT.

[63] The Office of Pipeline Safety is located in the DOT Research and Special Programs Administration (RSPA).

To enforce the pipeline standards, DOT may request the Attorney General to bring a civil action in an appropriate district court of the United States, and that court may award appropriate relief, including punitive damages. In addition, DOT can, after written notice and an opportunity for hearing, find a regulated entity in violation of the PSA and impose a civil penalty of not more than $25,000 per violation or for each day of violation, not to exceed a total penalty of $500,000.

DOT is also authorized under the PSA to conduct research and studies. For instance, under the Accountable Pipeline Safety and Partnership Act of 1996, DOT is to survey and assess the effectiveness of remotely controlled valves to shut off the flow of natural gas in the event of a rupture. DOT will determine whether the use of remotely controlled valves is technically and economically feasible and would reduce risks associated with such a rupture. If so, DOT will prescribe standards for use of these valves by interstate natural gas pipeline operators.

5.2.2.2 Environmental Protection Agency

The Clean Water Act (CWA; 33 U.S.C.A. § 1321) authorizes the EPA to regulate owners or operators of any off-shore or on-shore facility that could reasonably be expected to cause substantial harm to the environment by discharging oil into or on navigable waters or adjoining shorelines. These regulations (40 CFR 112 *et seq.*) apply to owners or operators of non-transportation-related on-shore and off-shore facilities engaged in drilling, producing, gathering, storing, processing, refining, transferring, distributing, or consuming oil and oil products.[64] In general, the regulations require regulated facilities to prepare and implement a spill prevention control and countermeasure plan, designed to provide for prompt emergency response and notification to authorities in the event of a spill.

5.2.2.3 U.S. Department of Energy

DOE was created in 1977 by the Department of Energy Organization Act of 1977. The Act consolidated many energy-related functions of the federal government into a single, Cabinet-level organization. DOE sets national policy concerning oil and gas production, supply, and distribution, including response to an energy crisis. It has emergency powers to allocate oil or natural gas to regions affected by a shortage and to increase production. For instance, during the Gulf War, DOE requested production states to act to lessen the impact of any disruption of

[64] These regulations do not apply to any on-shore or off-shore facilities that, because of their location, could not reasonably be expected to discharge oil into or on the navigable waters or adjoining shorelines. This determination must be based solely on consideration of the geographical, locational aspects of the facility and shall exclude consideration of human-made features such as dikes, equipment, or other structures. They also do not apply to transportation-related facilities that are subject to the authority and control of DOT, nor do they apply to facilities that do not have at least 42,000 gallons of underground buried oil storage or at least 1,320 gallons of aboveground oil storage. (49 CFR 192.5)

supplies due to Iraq's invasion of Kuwait. In response, the Texas Railroad Commission issued an emergency statewide rule (Statewide Rule 87, September 1, 1990) to allow oil wells to increase production over the state's normal production allowances up to each well's capacity for the months of September, October, and November.

DOE also operates the Strategic Petroleum Reserve (SPR). The SPR was created in 1975 by the Energy Policy and Conservation Act (EPACT) (Pub. L. 94-163, 89 Stat. 882, 42 U.S.C.A. 6234) in response to the oil crisis of that period. The Act was amended in 1992 to enlarge the SPR to one billion barrels. The SPR is an important resource for managing oil supply. The oil is located at various storage locations throughout the United States. The SPR is designed to minimize the impact of any interruption or reduction in imports of refined petroleum products and residual fuel oil. Congress can authorize DOE to sell this supply when market conditions dictate such action. During the Gulf War, the DOE did draw down some portion of the SPR to provide additional oil supplies. When the decision is made to use the SPR, DOE sells oil from it according to a formula set forth in DOE regulations (10 CFR 625).

The DOE can conduct sales and begin physical delivery of oil to purchasers in approximately sixteen (16) days following the Presidential decision to draw down. However, it may take weeks for purchasers to transport, process and deliver oil to consumers. Under Section 101(a) the Defense Production Act of 1950, DOE can obtain equipment needed for repair of damaged oil production facilities or expedite delivery of fuel oil to electric utilities, however, the exercise of such authority requires a Presidential declaration of national defense emergency (64 Stat. 798; 50 U.S.C.A. Appx §§ 2061, 2062, 2071. Also see E.O. 12038, February 3, 1978). Under the NGPA, DOE has been delegated the power to make emergency purchases and to allocate natural gas to high-priority users (E.O. 12235, September 3, 1980). DOE can also order pipelines to transport gas or construct emergency facilities. To activate these special powers, the President must declare a natural gas supply emergency. However, this emergency powers legislation may need to be revisited due to a restructured natural gas industry. (See *Energy Emergency Response Activities*, DOE Office of Emergency Management, Washington, D.C., May 1997)

5.2.2.4 Illinois Commerce Commission

In general, ICC (the Commission) regulatory supervision of public utilities focuses on setting the rates for service to customers. Most of the Commission's investigatory powers and prescription of rules and regulations concern the economic efficiency and prudency of the utility rather than public health and safety. (See the detailed discussion of ICC powers and authorities in Section 3.2.2.4 above.) However, under the Illinois Gas Pipeline Safety Act (220 ILCS 20/1 *et seq.*), the Commission is also authorized to implement a program of safety standards for pipelines within the state. Basically, the Commission adopts the minimum safety standards promulgated by DOT (83 Illinois Administrative Code 590). In addition, whenever the Commission finds a particular facility to be hazardous to life or property, it may require the person operating the facility to take steps necessary to remove the hazard.

The Commission also has the authority to investigate all accidents resulting in loss of life or injury to a person or property arising from a utility's maintenance or operation. Under the Illinois Pipeline Safety Act, the Commission requires pipeline operators to file reports of all accidents. Any accident report filed with the Commission is admissible into evidence in any action for damages arising from the accident.

The Commission can issue administrative orders to require public utilities to comply with the Public Utilities Act or any rule, regulation, or order issued by the Commission. If the utility does not comply with such an order, the Commission may file an action or proceeding in the appropriate Illinois circuit court. Any person who violates any provision of the Gas Pipeline Safety Act or any order, rule, or regulation of the Commission is subject to a civil penalty of not more than $1,000 for each violation for each date the violation persists. The maximum civil penalty may not exceed $200,000 for any related series of violations. In addition, the Commission may request an injunction to secure compliance. The Illinois Pipeline Safety Act does not specifically provide for criminal penalties.

5.2.2.5 Texas Railroad Commission.

The TRC has jurisdiction over any operation that involves:

- Drilling, operating, or producing oil, gas, or geothermal resources; brine mining injection; fluid injection; or oil and gas waste disposal wells;
- Transporting, reclaiming, treating, processing, or refining crude oil, gas and its products, or geothermal resources and associated minerals;
- Operating gasoline plants, natural gas or LNG processing plants, pressure maintenance or repressurizing plants, or recycling plants;
- Operating a pipeline; or
- Operating an underground hydrocarbon or natural gas storage facility.

The TRC exercises its economic regulation on the production of natural gas by setting production rates based on priority categories and the ratable share of market demand (16 Texas Administrative Code [TAC] 3.34). These production rate regulations are complex and established to prevent waste, including producing natural gas in excess of market demand, protecting correlative rights, preventing discrimination between different wells in the same field, and conserving the natural resources of Texas. In addition, the TRC requires each oil and gas producer to obtain approval for drilling wells, operating pipelines, operating LPG or CNG facilities, or constructing and operating underground hydrocarbon storage facilities.

The TRC is the agency certified by DOT to regulate the safety of natural gas and oil pipelines within the state. The TRC receives all reports of accidents and safety-related conditions for each facility under its jurisdiction.

The TRC has regulations providing for emergency response to shortages, including a means for each producer or purchaser to increase production from wells in a field in response to an increase in demand caused by unforeseen events. As discussed above, this was done in Statewide Rule 87 in response to Iraq's invasion of Kuwait. If economic inequities occur as a result of the production authorized in an emergency, the TRC may make an adjustment after a hearing.

5.3 Regulations and Critical Infrastructure Protection

5.3.1 Impact of Regulations on Critical Infrastructure Protection

Oil and Gas Pipelines and Equipment

The oil and natural gas supply systems may be vulnerable to criminal tampering at any point in the system: production wells and off-shore platforms, gathering lines, treatment facilities (i.e., refineries), transportation pipelines, compressing and routing stations, storage facilities, and consumer distribution mains. Because production facilities are numerous and widespread, it is unlikely that destruction of any particular facility would create a significant crisis in the oil or natural gas industry. For example, the destruction of a natural gas production well field could result in a serious fire emergency situation requiring immediate response and possible danger to adjacent properties; however, it would not create a national supply crisis. As another example, damage to an off-shore oil production well could result in a significant environmental emergency requiring immediate response and might result in public health, environmental, and economic impacts on local shorelines and the fishing/shellfish industries. But again it would not cause a significant supply crisis.

Most oil and gas pipelines are substantially protected from damage by being buried underground. In fact, the more populated the area, the deeper pipelines are required by DOT to be buried to prevent accidental harm to public health or property. The most vulnerable components of the oil and natural gas infrastructure would be aboveground compression and routing stations, large pipeline intersections, large pipeline interfaces (e.g., natural gas city gates), or large storage facilities. Of particular vulnerability are aboveground interconnections between interstate pipeline supplies and LDC distribution systems (city gates). Often only a small number of interconnections serve to supply gas to the whole distribution system, and without significant LDC storage facilities, the destruction of these city gates could disrupt gas service to a large number of residences and public buildings.

The following discussion addresses regulatory requirements for security at vulnerable facilities, along with requirements for emergency response in the event of spill, equipment failure, or fuel shortage.

There are clear, direct requirements for security systems or restricted access to certain vulnerable components of the oil and gas infrastructure. Although not designed for the prevention of intentional sabotage, the EPA regulations on spill prevention for oil storage and production facilities address facility security (40 CFR 112). For instance, the EPA regulations require all plants that handle, process, and store oil to be fully fenced and all entrance gates to be locked and/or guarded when the plant is not in production or is unattended. In addition, all flow and rain valves and any other valves that would permit the direct outward flow of a tank's contents must be securely locked closed. Starter controls on oil pumps must be locked. In addition, the facilities must have lighting that is commensurate with the type and location of the facility, specifically considering the prevention of spills occurring through acts of vandalism. The general requirements to prevent accidental spills, including secondary containment, leak detection systems, and automatic shut-off systems, may also serve to minimize the impact of an intentional release of oil to the environment or creation of a fire hazard.

Although designed for the prevention of accidental releases, pipeline safety regulations enforced by DOT and certified states provide some physical protection for pipeline operations from possible criminal intrusions. As mentioned above, DOT regulations for natural gas pipelines classify areas according to population density.[65] Pipelines constructed through more densely populated areas must meet stricter standards with regard to construction materials, depths, and other design factors (49 CFR 195.248). For oil pipelines, the regulations require pipeline rights-of-way to be selected to avoid, as far as practicable, areas containing private dwellings, industrial buildings, and places of public assembly (49 CFR 195.210). No pipeline can be located within 50 feet of a private dwelling, industrial building, or place of public assembly unless it is provided with at least an additional 12 inches of cover over the normal cover requirements. These construction and siting requirements make the pipeline less vulnerable to destruction in these areas where the greatest harm could result.

The regulations require more vulnerable aboveground natural gas compressor stations to be (1) located on property under the control of the owner/operator of the pipeline, (2) far enough away from adjacent property to minimize the possibility of fire moving between the compressor building and adjacent buildings, and (3) fenced (49 CFR 192.163). In addition, the buildings must be equipped with adequate fire protection facilities and appropriate shutdown or alarm devices in the event of equipment failure. Any aboveground oil facility (e.g., pumps) must be constructed in areas under the direct control of the operator of the pipeline and in an area inaccessible to the public (49 CFR 195.254). Valves must be installed so as to be protected from damage or tampering (49 CFR 195.258). Aboveground oil breakout tanks must be adequately protected against unauthorized entry, and oil pipeline pumping equipment must be equipped with emergency shutdown devices (49 CFR 195.264 and 195.436).

[65] Under DOT regulations, a Class 1 location has 10 or fewer buildings intended for human occupancy; a Class 2 location has 10-46 buildings; a Class 3 location has 46 or more buildings or is situated where the pipeline lies within 100 yards of an area where 20 or more persons gather (i.e., playground, outdoor theater, recreation area); and a Class 4 location is any location where buildings of four or more stories aboveground are prevalent (49 CFR 192.5).

DOT requirements also require each operator of a regulated natural gas or oil facility to have a manual of written procedures for conducting emergency response, including procedures for handling abnormal operations (49 CFR 192.605 and 195.402). Abnormal operations can include unintended closure of valves or shutdowns; increases or decreases in pressure or flow rates outside normal operating limits; loss of communications; and operation of safety devices. All of these abnormal operations could be caused by normal equipment failures, natural disasters, or criminal activity. The operator's response, however, would be the same. Under the requirements, the operator must investigate and correct the cause of the abnormal operation, including checking sufficient critical locations in the system to determine the continued integrity and safe operation of the pipeline, even after the abnormal operation has ceased.

LNG Facilities

Special DOT regulations govern the operation of LNG facilities used in the transportation of gas by pipeline (49 CFR 193.2001 *et seq*). LNG facilities could possibly be vulnerable to hostile action because of the volatile nature of LNG and its ability to disperse in a dangerous (explosive) vapor-gas cloud. DOT regulations require all LNG container and transfer system facilities to use a specific formula to determine a dispersion exclusion zone. Within this zone, there may be (1) no outdoor area occupied by 20 or more people during normal use (e.g., beaches, playgrounds, other recreations areas), (2) no residence or other building occupied by 20 or more persons in normal use (schools, commercial establishments, etc.), and (3) no facility containing explosive, flammable, or toxic materials in hazardous quantities or that could be an additional hazard if exposed to a vapor-gas cloud. In addition, the facilities must be equipped with separately routed or underground local, remote, and redundant signal lines for all control systems that affect any operational component that is not otherwise fail-safe.

There are very specific security requirements for LNG facilities. Security personnel must be trained in their duties, including actions to be taken and notification to be made whenever there is any indication of an actual or attempted breach of security. Access to the plant must be restricted, and positive identification of all persons entering is required. Vulnerable facilities (e.g., storage tanks, transfer system, process equipment, control rooms and security communications systems) must be surrounded by a protective enclosure, and the enclosure must be located such that features outside the facility (e.g., trees, poles, buildings) cannot be used to breach the security of the enclosure. All enclosures must be locked unless continuously guarded and sufficiently illuminated. The protective enclosure must be of sufficient strength and configuration to obstruct unauthorized access to the facilities, including 7-foot-high fencing with at least one foot of barbed or similar topping. Security procedures must include the use of direct communications between all on-duty security personnel and all control rooms and stations. Each enclosure must be monitored for the presence of unauthorized persons, either by visual observation on a schedule or by security warning systems that continuously transmit data. In addition, security equipment must have an alternative power source.

The regulations also require emergency planning, including emergency evacuation plans. Emergency response procedures must consider the worst-case discharge volume and the potentially affected environment.

Role of Planning and Procedure

Emergency planning is not a way to prevent attack on the oil or natural gas infrastructure but is critical in minimizing the impacts of such attacks. Planning is performed for short-term, immediate response and for longer-term cleanup. Probably the most critical emergency response planning is for the resumption of natural gas or oil service after an equipment or facility failure. The ability to bypass vulnerable facilities and still move the product to the end user will minimize or eliminate any significant impact on the infrastructure from the destruction or immobilization of a critical facility.

As discussed above, both oil and gas pipeline operators must have a manual of written procedures that address the response to abnormal operations (loss of important facilities or equipment). In addition, oil pipelines must have an oil spill response plan to reduce the environmental impacts of an oil discharge (49 CFR Part 194). The response plans must determine the worst-case discharge for each response zone (49 CFR 194.105). This planning must include procedures for repairing pipeline facilities and starting up and shutting down any part of the pipeline in a manner designed to assure operations within the maximum allowable operating pressure limits prescribed in DOT regulations. It requires that personnel have the ability to isolate portions of the system to allow for repairs. The regulations require the operator to periodically review the response of operating personnel to determine the effectiveness of the procedures for controlling abnormal operations and taking corrective actions when problems are found. Procedures are in place to ensure the continued operation of a critical facility, even in a diminished state. As long as the natural gas or oil can be transported to the end user, the infrastructure continues to function.

In addition, under the NGPA, the President has authority to declare a natural gas supply emergency upon finding that there is a shortage threatening high-priority uses (e.g., space heating in winter). Pursuant to Executive Order 12235, the President has delegated emergency powers under the NGPA to DOE. (September 3, 1980, 15 U.S.C.A. § 3363 note). Under the emergency powers, once the President has declared an emergency, DOE may authorize any interstate pipeline or LDC served by any interstate pipeline to contract, upon such terms and conditions as DOE determines to be appropriate, for the purchase of emergency supplies of natural gas. DOE may also require any interstate pipeline to transport the natural gas for the contract purchaser. DOE may also allocate natural gas supplies to any interstate pipeline or LDC served by a interstate pipeline for the provision of high-priority gas uses. The Executive Order provides that DOE must consult with the EPA and the Federal Emergency Management Agency (FEMA) in exercising these emergency functions.

It should be noted that although this authority exists, the subsequent deregulation of the natural gas industry, resulting in greater pipeline utilization, may make it difficult to redirect gas on an emergency basis.

5.3.2 Measures for Improvement

Review of the current regulatory scheme for oil and natural gas production, transport and distribution suggests the following areas for consideration in terms of improvements to infrastructure security.

1. *Develop systemwide contingency planning*. Deregulation has created a competitive interstate market for producers and transporters, who must now become efficient and cost-effective to meet competitive pressures. This effort may include filling pipelines to capacity with consumer shipments, thereby reducing excess capacity for use during an emergency when rerouting is necessary. It may be worthwhile to encourage industry members to use the existing associations to develop a reliability plan, after the pattern of the North American Electric Reliability Council (NERC). Possibly FERC or DOE, as energy-policy-making bodies, could work with the National Petroleum Council (NPC), American Petroleum Institute (API), Interstate Natural Gas Association of America (INGAA), American Gas Association (AGA), and Gas Research Institute (GRI) to establish an integrated, cooperative contingency planning system.[66]

   It may also be worthwhile to work with these groups to develop contingency procedures for quick access to the SPR. With the current trend toward fewer production facilities and reduced domestic production, the United States will become more dependent on foreign oil. This reduction in domestic facilities may mean that sabotage to a small number of domestic production facilities will have a greater impact on infrastructure and continuous delivery. Although the SPR provides backup reserves in case of shortage, due to the regulatory requirements concerning the sale process for these supplies, it may be difficult to quickly disburse these reserves in emergency situations. The SPR was established to react to gradually increasing supply shortages (e.g., the discontinuance of foreign supplies due to political difficulties) rather than an immediate loss of supply to a region (due to the immobilization of the production or transportation infrastructure).

2. *Include sabotage scenarios in the development of risk management plans.* New legislation contemplates using risk management plans to examine pipeline vulnerabilities. Under this system, for infrastructure security concerns to be addressed, hostile action scenarios must be considered in the risk analyses. DOT should work with industry so that

[66] See Natural Disasters and the Gas Pipeline System, GRI-96/0385, Gas Research Institute, Chicago, Illinois November 1996. The API already issues recommended standards in various areas, including safety and fire standards, environmental and health issues, measurement standards, and other categories of interest to its members.

the requirements for these risk management plans are clearly laid out and that planning for sabotage is considered in the initial development of the risk models.

3. *Consider effect of fragmented jurisdiction*. Finally, it should be noted that the fragmentation of regulatory authority in this area may create obstacles to implementation of any new initiatives. Federal regulation of the industry is split among DOE, FERC, DOT, EPA, and the Coast Guard. Moreover, many safety requirements are enforced at the state level. Except for DOT pipeline safety standards, which are adopted by state agencies for implementation on the state level, changes in state regulation of the oil and natural gas industry would also require reforms addressed to PUCs, pipeline-safety-certified agencies, and other oil or natural gas production regulatory bodies in 50 states.

[This page intentionally left blank.]

6 BANKING AND FINANCIAL SERVICES

6.1 General Description of Regulation

Our economy depends on a healthy banking and financial services sector. Regulation of this sector is intended to promote economic stability and growth by: (1) protecting depositors and investors; (2) providing a steady source of funds for investment in economic ventures; (3) maintaining a stable currency; and (4) providing an atmosphere of stability, trust, and legal enforcement that will foster the conclusion of financial transactions. These have always been the goals; the methods of achieving them have evolved over time. The overview below provides a brief outline of the financial services sector, the types of regulation that are applied to it, and how the regulatory system has developed in response to various crises.

6.1.1 Current Regulatory Environment

Description of the Banking and Financial Services Sector

Banking

Banks are the primary institutions for holding, lending, borrowing, and circulating money. The essential economic characteristic of banks is the creation of credit. In the United States, banking is generally thought of as consisting of two parts; commercial banks, whose main functions are accepting deposits and creating credit through short-term loans, and investment banks, which primarily underwrite and sell new issues of stocks and bonds to investors. When acting in the role of underwriter, a bank guarantees to furnish a definite sum of money on a specific date in exchange for a given number of bonds or shares of stock.

From the 1930s until recently, the United States has not allowed banks to perform both commercial and investment banking functions under one charter. The functions had to be managed under separate ownership and control. Additionally, banks have not been allowed to provide other types of financial products or services, such as insurance or brokerage. Provision of these products and services has been restricted to the financial services houses, traditionally outside the sphere of banking in this country.

Financial Services

Brokerage houses and financial services institutions deal in the transfer of risk, equities, and expectations from one holder to another. The major types of transactions are:

- *Insurance*. The most obvious risk-transfer transactions are those involving insurable risk. Daily, billions of dollars discount to other parties willing to purchase and hold them.

These transactions cover far more than the familiar fire, flood, theft, or life insurance; they also include the vast sums needed to reduce the risk of commerce, such as business interruption, goods-in-transit, accounts receivable collection, and so on. This is a fiercely competitive industry, and the timeliness and accuracy of information is crucial. The entire industry has placed as many of its activities on-line as can be accomplished within the boundaries of safety and security.

- *Equity*. Equity transfers in the United States are best exemplified by the trading on the major exchanges. While the law still requires that shares of stock, bonds, and debentures have a physical manifestation, trading in the *value* of these pieces of paper occurs without the items being present or even visible. One exchange, the National Association of Securities Dealers' Automated Quotation System (NASDAQ), is a virtual exchange, in that even the traders are present only in cyberspace. Trillions of dollars are represented only by the contents of computer files. The timeliness, accuracy, and security of these files is the basis of trust on which the industry operates.

- *Commodities*. While the trading of commodities is often thought of as buying and selling large quantities of goods and materials, it is actually a means of transferring expectations about the future from one holder to another. These transfers entail agreements as to the quality, quantity, time, and location of delivery of grain, lumber, building materials, petroleum and petroleum products, and financial obligations — all items for which actual delivery is to occur in the future. Many farmers, bankers, insurers, manufacturers, wholesalers, and retailers use this industry to "insure" against the uncertainties of life and commerce. Huge sums are traded daily from those who believe that the subject items will increase or decrease in the future to those who hold opposite expectations. All of these transactions are virtual, in that very few participants in the trading of commodities ever expect to actually make or take delivery. As these markets have become global, with trading continuing around the clock and around the globe, the timeliness, accuracy, and security of the information flow are of paramount concern.

Settlement of transactions conducted in any of these industries is conducted primarily by privately owned and operated entities, such as the National Securities Clearing Corporation, Depository Trust Company, Government Securities Clearing Corporation, and International Securities Clearing Corporation. While these entities maintain high standards for security and accuracy, determined individuals have penetrated their databases for brief periods. Although no major losses of funds have occurred, the industries and the attendant settlement entities must be constantly vigilant as new technologies are available to a wider number of users.

As with other firms dealing in electronic funds transfer, a significant issue for the members of these industries is the authentication of who owns the value represented and who has authority to make changes in that ownership.

Current Regulatory Techniques

Techniques of Banking Regulation

Banking regulation in large part consists of measuring the financial health of banks. When a bank is identified as being at risk of failure, generally regulators first attempt to encourage a private industry solution, such as acquisition by another (stronger) bank. As a last resort, the Federal Deposit Insurance Corporation (FDIC) provides protection for depositors (see Section 6.2 below). To make their financial health measurements, regulators have adopted rules, generally centered on the elements of what has become known as the "CAMEL" rating. CAMEL is an acronym for the accepted indicators of performance of commercial banks:

- Capital adequacy,
- Asset quality,
- Management competency,
- Earnings, and
- Liquidity.

Banking examiners have published rules establishing ratios by which an institution is rated. A CAMEL rating of 1 is good and 5 is bad.

Banking regulation is also an essential part of the management of the national economy; regulations on banks are the tools used by the government to regulate the availability and cost of credit. Such regulatory tools include regulations on (1) the portion of deposits held on demand by banks, which must be retained in available cash ("reserves"); (2) the discount that the central bank (the Federal Reserve System) requires from banks that must sell securities to cover demands for cash that cannot be met immediately from reserves ("rediscount rate"); and (3) the interest rate that the central bank charges other banks for short-term loans to ensure liquidity ("funds rate").

Techniques of Financial Services Regulation

For the investment side of the financial services industry, statutes, case law, and regulatory practice have resulted in a standard that is balanced between protecting the investor from fraud and deceit and promoting the free exchange of value among ready, willing, and able buyers and sellers. The underlying principle is that of full disclosure. Regulators cannot directly set the exchange rate for representations of value[67]; the investor or purchaser must make that decision. Regulators can act only to insure that no relevant facts are intentionally withheld from buyers and sellers. This balance between supporting the market and protecting participants has been maintained by focusing on the following elements of financial services:

[67] A "representation of value" is something *other than* cash, coin, or bullion that can be converted, at a rate determined by comparison with a known numneraire, into another such representation, or exchanged for goods, services, or for a claim on goods or services. Such a representaion can be physical (e.g., paper or plastic) or nonphysical (e.g., electronic).

- *Products.* Representations of value that are offered to the public must be registered with federal agencies, state agencies, or both.

- *Practices.* Regulators attempt to prevent (1) misleading or false inducements to buyers and sellers and (2) manipulation of value by persons with fiduciary or insider status superior to that of those to whom financial products are sold.

- *Prices.* Regulations directed at limiting excessive or inflated pricing of representations of value (which set limits on interest rates, service fees, and other transaction costs) are intended to ensure that the price paid for a representation of value accurately reflects the real underlying value and is not inflated by fraud or excessive hyperbole.

Evolution of Banking and Financial Services Regulation

When the United States was formed, there was no constitutional provision for a national banking system. The founders of the new nation were very much aware of how the European nations had suffered from the inflationary practices of their national banks in financing wars and colonial expansion. They believed that leaving all banking activities in the hands of private merchant-bankers would prevent those excesses.

During the War of 1812 and the War between the States, the nation faced serious difficulties in obtaining needed credit at reasonable rates. By 1863, the need for a national banking system to provide a means to discipline the many state-chartered banks and satisfy the credit needs of a growing nation was obvious. Congress studied the crises that arose after the charters for the First and Second National Banks were allowed to expire. The result was legislation[68] that attempted to balance the demonstrated need for a national banking system and the fears of a populist-minded Congress of placing too much power in the hands of a few financial czars. This legislation created the Office of the Comptroller of the Currency (OCC), which was made responsible for chartering and supervising national banks owned by private parties. Those forming a national bank were required to purchase U.S. government bonds in amounts equal to one-third of their capital and place these bonds on reserve with the Treasury Department. This meant that the bank's reserves would be backed by the full faith and credit of the federal government.

In 1907, the nation faced another banking crisis. Many of the national banks under the supervision of the OCC and most of the state-chartered banks were caught with seriously short cash reserves when railroad and mining stocks fell. When one bank was unable to meet a depositor's demand for cash, other banks faced a loss of confidence, and they too were subject to a run on their reserves. This chain reaction led to many bank failures and a general loss in confidence in the banking system. Following a public outcry to address this crisis, Congress

[68] The Currency Act of 1863 and the recodification in the National Bank Act of 1864 (Chap. 106, 13 Stat. 99).

studied the situation for five years, then decided that the national system of supervision needed to be buttressed with a national system of bank reserves that could react quickly to expand or contract the supply of money (credit) to stabilize the need for cash and commerce. Beginning with a Congressional Resolution in 1912 and legislation in 1913, the National Reserve Association (later the Federal Reserve System[69]) was created. It had 12 banks and district branches around the country and authority to mobilize cash reserves, issue credit to national banks, and state-chartered banks who choose to become members, and oversee the required Treasury balances. This legislation also added an incentive for state-chartered banks to join the Federal Reserve System (the Fed) as an alternative to seeking a federal charter. Membership in the Fed allowed state banks to get the same discounts for short-term loans as did federal banks. State banks that joined the Fed had to submit to reserve limits and supervision overseen by the Federal Reserve Board. National banks were automatically members of the Fed, but their supervision remained with the OCC. So in 1913, Congress had dealt with the problems behind the politically sensitive issues of the day, but in 15 years, another crisis was to bring banking back to the front political burner.

After the 1913 act, banks were still allowed to act directly as investors and underwriters of commerce and business expansion. As the fervor of investment in railroads, mines, and the like began to be franchised among banks across the country, control of regional investment potential became a hot political subject. In 1927, smaller Western bankers were successful in getting a bill passed that barred interstate banking.[70] This left the states with the onus of controlling the rampant speculative investments by nonfederal banks. When more than 9,000 commercial banks failed between October 1929 and late 1933, pressure was again put on Congress to do something. Again, Congress studied the situation through a series of investigations and hearings, followed by passage of legislation that:[71]

1. Created a national system of insurance on deposits;

2. Prohibited commercial banks from engaging in offering securities to their depositors, and

3. Prohibited all commercial banks from engaging in investment banking activities.

The Securities and Exchange Act of 1933 established a mechanism for supervising the noncommercial banking institutions now permitted to act as underwriters and offer securities to the public; the goal was to ensure informed investment and prohibit any fraud in inducing people to purchase securities. In 1934, another Securities and Exchange Act broadened the mandate for disclosure of information pertinent to investors, by forcing brokers to disclose who was "behind" each deal and what stake they had in it and to provide some statement about risk factors that should be considered by investors. The temporary depositor insurance was made permanent and

---

[69] The Federal Reserve Act of 1913 (Pub. L. 63-43, 38 Stat. 251, 12 USC 221).

[70] The McFadden Act of 192, (Pub. L. 69-639, 44 Stat. 1224).

[71] The Glass-Steagall Act of 1933.

placed under the supervision of the FDIC in 1935. The FDIC was also given the additional responsibility of supervising those state-chartered banks that received FDIC insurance coverage but did not join the Fed. Thus, by the beginning of World War II, the nation's laws controlling banking and financial services were as follows:

- National Banking Act of 1864 (established federally chartered banking)
- Federal Reserve Act of 1913 (established the Federal Reserve System),
- McFadden Act of 1927 (prohibited interstate banking)
- Glass-Steagall Act of 1933 (established the FDIC and separated types of banking),
- Securities and Exchange Act of 1933 (established the Securities and Exchange Commission disclosure requirements), and
- Securities and Exchange Act of 1934 (broadened disclosure requirements).

By the end of World War II, the nation had a bank regulatory system organized as shown in Table 6.1.[72]

Federal regulation of the issuance, sale, and trade in securities was solely the province of the Securities and Exchange Commission.

All activities involved in banking and financial services at that time were based on paper, gold, silver, and direct exchange between human agents. The only electronic media involved were the ticker machine for stock quotes and telephones for making deals.

This structure prevailed into the 1980s, even though the adoption of electronic banking and trading had already vastly changed the rate at which this industry was evolving. Banks and bank holding companies had begun to acquire competitors and consolidate operations that could be done more efficiently by the mainframe computers that were rapidly becoming available. The early versions of today's electronic funds transfer systems were established as part of this expansion. Although Congress did pass legislation in 1956 to require the Fed's approval to establish a bank holding company and prohibit such holding companies from interstate branching,[73] the electronic "cat" was out of the bag. A system that was developed to deal with crises occurring during the first half of the 20th century was faced with new and different problems in the second half.

---

[72] This chart and the following discussion of the three regulatory agencies is drawn from Anne M. Khademian, *Checking on Banks: Autonomy and Accountability in Three Federal Agencies*, The Brookings Institution Press, Washington, D.C., 1996.

[73] Financial Institutions Regulatory and Interest Rate Control Act of 1978 (Pub. L. 95-630, 92 Stat. 3641).

Table 6.1 Bank Regulatory Agencies from the Late 1940s to the 1980s

Characteristics	Regulatory Agency		
	OCC	Federal Research Board	FDIC
Supervisory Jurisdiction	National Banks	State-chartered banks that belong to the Federal Reserve System and bank holding companies	All other state banks that are covered by Federal Deposit Insurance
Agency type	Bureau within the Treasury Department	Independent agency	Government-chartered corporation
Regional and Field organization for supervision	Six districts that oversee duty stations	12 Reserve Banks	Eight regional offices that oversee field offices
Mandates other than supervision	Administration of the national banking system	Regulation of the money supply	Management of the Bank Insurance Fund

Before the laws were revised in the last two decades, the three regulatory agencies took very different approaches to their responsibilities. Each adopted a different blend of *regulation* versus *supervision*. A strict regulatory approach emphasizes compliance with measurable standards of performance and risk management. A supervisory approach emphasizes safety and soundness of banks as determined by the guided judgment of bank examiners.

The Fed relied on its expertise as the nation's central bank and its independence from political demands. Its examiners followed a strict regulatory approach. They conducted a full examination of every bank under the Fed's jurisdiction every year. These examinations were intended to determine the degree to which a bank was in compliance with strict regulatory mandates for capital reserve, risk management, and other quantifiable measures of safety.

Examiners in the OCC, as a part of the Executive Branch, were given far more leeway to use their judgment in taking a supervisory, versus a regulatory approach. The OCC relied on a concept of hierarchy of risk. Examiners focused on practices related to systemic risk, which included activities posing a threat to the entire industry and on large, regionally important banks, whose difficulties have systemwide impact. Not every bank was examined regularly, and only troubled banks were examined every year.

The FDIC fell somewhere in between the patterns of the Fed and OCC. Its examiners applied

strict risk management standards for certain classes of bank activities, but conducted much of their examination off-site by review of reports and documentation submitted regularly by the banks. On-site examinations for strict compliance were conducted at about two-thirds of supervised banks.

As the nature of banking began to change with the introduction of new communications and computing technology, Congress tried to keep the regulatory environment in step with those changes. The Financial Institutions Regulatory and Interest Rate Control Act of 1978[74] created major statutory provisions regarding electronic fund transfers and created the Federal Financial Institutions Examination Council (FFIEC) to begin bringing standard practices to the regulatory bodies. The Depository Institutions Deregulation and Monetary Control Act of 1980 eliminated interest rate ceilings for savings and time deposits and raised the level of FDIC insurance coverage to increase the competition among depository institutions. The three regulatory bodies were, however, given much freedom to conduct their business as they saw fit until the system faced another crisis.

The number of bank failures suddenly jumped from the 5 per year level that occurred in the period 1933 - 1986 to 200 per year in 1987. The Federal Deposit Insurance Fund showed a negative balance of $7 billion in 1991. Once again, Congress addressed the crisis through a process of hearings and legislation.

The Financial Institutions Reform, Recovery, and Enforcement Act of 1989[75] gave thrift institutions (savings and loans) coverage under FDIC insurance and created the Federal Housing Finance Board (FHFB) and the Office of Thrift Supervision (OTS) to oversee these now federally insured institutions. This act also created the Resolution Trust Corporation (RTC) to manage failed or troubled institutions that regulators took over under the insurance provisions. The Federal Deposit Insurance Corporation Improvement Act of 1991 limited the discretion that federal supervisors from the Fed, OCC, and FDIC had previously exercised in assessing the condition of banks and determining what enforcement actions were needed. Congress wanted certain responsibility for ensuring that the national system of banking is well-managed, and they wanted the federal regulators to shoulder that responsibility.

In addition to responding to the bank failure crisis, Congress also had another specter to cope with: competition from huge foreign banks for financing new ventures and industrial growth. Restrictions on interstate banking and vertical integration put U.S. banks at a disadvantage.[76] Congress eased those restrictions by repealing part of the Glass-Steagall Act and allowing banks to grow larger and branch across state lines, subject to concentration limits, state laws, and evaluation of the companies.[77] Further changes in the law allowed bank holding companies to

[74] Pub. L. 95-630, 92 Stat. 3641.

[75] Pub. L. 101-73, 103 Stat. 183.

[76] See, for example, BankNet Electronic Banking Service at http://mkn.co.uk/bank.

[77] Riegle-Neal Interstate banking and Branching Efficiency Act of 1994 (Pub. L. 103-328, 108 Stat. 2338).

own more than one kind of banking enterprise, so that small banks and mortgage lending institutions began to be combined under centralized regional management. However, such combinations are potentially subject to regulation by many agencies. This has led to situations, for example, where the various parts of a small regional bank holding company must adhere to the banking rules of the Fed and FDIC, the banking rules of four states, and the mortgage lending rules of at least five states. As one banker put it, "I see more teams of examiners in my office every year than I do baseball teams on television."[78]

6.1.2 Current Trends in Regulation

Electronic commerce is a reality in banking and financial services, and it poses some serious problems for regulators. The following brief discussion is intended to provide an overview of the major vehicles of electronic commerce, and the new challenges they pose to regulators. The impact of these systems on critical infrastructure protection is discussed in Section 6.3.1.

Electronic Funds Transfers (EFT)

This term refers to the movement of funds from one bank account to another by means of electronically communicated payment instructions. It has been estimated that each day, banks, global financial markets, and the U.S. Federal Reserve transfer more than $35 trillion within, into, and out of the United States. Citibank alone transfers $500 million daily, including domestic transfers. Recently, Citibank worked with domestic and foreign law enforcement agencies to track and trap a group of criminal hackers who, before they were caught, had transferred $400,000 into several foreign accounts. The crimes went unnoticed for several months because the transfers were kept small and below set limits for investigation. It was only when the crooks got greedy that they were found out.

Electronic Checks

Several major banks have fully instituted paperless checking as an option for payments over the Internet. Basically, this system transmits the same data that is contained in paper checks, but in machine-readable format. Businesses and individuals use this system just as they do paper checks, except that each check bears a digital rather than manugraphic, signature for signing, endorsing, and authentication. The effective and safe use of these systems will require highly secure and reliable management of the electronic signatures.

Digital Cash or Tokens

[78] Remark made not-for-attribution during an interview.

Any electronic representation of money in digital form can be negotiated and transmitted among payers, payees, depositors, and depositories. Stores of such digital cash or tokens — held in on-line accounts, smart-cards, or "electronic wallets" (palm-sized PCs) — can be presented, transferred, and negotiated just like currency. There is no need for an intermediary, as there is for electronic checks or credit cards. The repository can be "recharged" on-line, at an ATM, or by a teller. Digital cash can be "identified" and carry data about the person to whom it belongs, or it can be anonymous. The same caveats regarding electronic signatures that apply to electronic checks apply to digital cash. In addition, a major threat resulting from widespread use of anonymous digital cash or tokens is the ease by which money can be laundered in this format. As the U.S. Treasury Financial Crimes Center has stated:

> These systems are designed to provide the transacting parties with immediate, convenient, secure and potentially anonymous means by which to transfer financial value. When fully implemented, this technology will impact users worldwide and provide readily apparent benefits to legitimate commerce, however, [it] may also have the potential to facilitate the international movement of illicit funds.[79]

A significant issue for financial institutions in coping with all of these computer-based systems is authentication of who owns the value represented, and who has authority to make changes in that ownership. What is really needed is a way to identify those who transact business using electronic money, just as we attempt to do with those using paper-based currency — have the transactor show some identification.

There is currently a struggle between elected officials, particularly those in Congress, and the regulatory agencies. The elected officials are again under pressure to do something, and this time their answer is to make regulatory agencies more accountable for the health and safety of the banking system. Their prescription is to consolidate the regulatory agencies and strictly codify the standards and procedures, reducing the numbers of both regulations and regulators. Those who manage the regulatory system have a different solution: greater autonomy for examiners and less reshuffling and reorganization of authority and responsibility. The trade-off is between accountability and flexibility.

This struggle over accountability versus flexibility is taking place just as the nation faces the potential for another crisis in banking and finance. The lines between banking and non-banking financial services such as investment counseling and brokering, insurance, and investment banking are under attack. The attack is driven not merely by those who stand to gain from

[79] "Money in cyberspace," at http://www.ustreas.gov/treasury/bureaus/fincen/cybpage.html #concern.

consolidation of such services; it is also the result of demands from the public, who want to have access to a full range of financial services and products with as little change in venue and "user interface" as possible.[80]

With substantial changes in banking infrastructure due to increase competition, new technology, and the amendment and revision of the law in the latter part of the 1990's, the banking environment of the United States is entering a period of dynamic change. The regulatory scheme that was present in 1975 will probably not be evident in the system of 2010. While the same federal agencies have the same compartmentalized responsibilities today, it is likely that dramatic changes will be made as changes in the industry render old regulatory methods obsolete.

6.2 Description of Selected Regulatory Agencies

6.2.1 Selection Method

The federal agencies profiled below represent the primary agencies involved in regulation of banking and financial services. Following the discussion of federal agencies is an overview of the general practices among state regulatory agencies. The state overview is not intended to represent any specific state but rather to illustrate the range of regulatory goals and techniques applied at the state level.

6.2.2 Agency Descriptions

6.2.2.1 Federal Agencies

The roles of the federal agencies that oversee the banking and financial services industry all have their origins in previous crises in commercial or investment banking.

<u>Bank Regulation</u>

The roles of the three basic federal banking regulatory agencies are shown in Table 6.1 above. Table 6.2 below summarizes key features of three additional agencies that have been created or whose roles have expanded since 1987 in response to the crisis in thrift institutions.

[80] See, for example, 1997 Senate Bill 377, "Promotion of Commerce On-Line in the Digital Era."

Table 6.2 Recently Created or Expanded Bank Regulatory Agencies

CHARACTERISTICS	FFIEC	OTS	FDIC
Supervisory jurisdiction	National Banks	All thrift institutions insured by FDIC	Also insures deposits of thrift institutions
Agency type	Independent agency	Office within Treasury	Government-chartered corporation
Regional and field organization for supervision	Works through FED districts and state regulators	Works through FED districts and state regulators*	Eight regional offices that oversee field offices
Mandates other than supervision	Helps oversee systems for electronic funds transfers	None	Management of the Bank Insurance Fund.

A brief summary of the responsibilities of the selected federal agencies follows.

- *The Fed*. The Fed is an independent agency with the responsibility for regulating the nation's supply of money, and supervisory jurisdiction over all state-chartered banks that belong to the Federal Reserve System. The Fed can mobilize cash reserves, issue credit to national banks, and oversee the required balances.

- *OCC.* The Office of the Comptroller of the Currency (OCC), a bureau in the Department of the Treasury, is the administrator of the national banking system. As such, the OCC has supervisory jurisdiction over all federally chartered banks.

- *FDIC.* The Federal Deposit Insurance Corporation (FDIC) is a federally chartered corporation that manages the Bank Insurance Fund. In that role, the FDIC insures deposits in all federally chartered banks, state-chartered banks that join the Federal Reserve System, and all thrift institutions eligible for the insurance fund. The FDIC also has supervisory responsibility over state-chartered banks that choose to be insured by the Bank Insurance Fund but not to join the Federal Reserve System. The FDIC also resolves and liquidates failed banks covered by the Bank Insurance Fund.

- *OTS.* Another agency of the Treasury Department, the Office of Thrift Supervision (OTS) oversees all thrift institutions insured by the FDIC. The OTS resolves and liquidates all failed thrifts under its supervision.

- *FFIEC.* The Federal Financial Institutions Examination Council (FFIEC) is a coordinating body, created to standardize practices among the regulatory agencies regarding national banks. It has a strong role in overseeing the systems for electronic funds transfers.

Investment Regulation

The Securities and Exchange Commission (SEC) oversees the persons and institutions that offer stocks and bonds to the public. This oversight includes licensing and registration of dealers and brokers, registration of securities, investigation of alleged fraud or misleading practices, and requirements for internal controls for institutions engaged in investment banking.

6.2.2.2 State Agencies

The state agencies go by varied and sometimes confusing names. Some states combine all financial services and banking under a State Banking Commissioner; others have separate offices to supervise banks, thrifts, and securities firms. All supervise credit unions separately, although sometimes under a broader umbrella. A summary of the stated purposes and goals of state regulation follows.

Source of Authority

The basis for most state banking and financial services regulation is constitutional authority implemented by legislation. The legislation often includes many pages defining the exact nature of the things to be regulated. Most of these definitions are concerned with the institutions and their products and activities that are to be the subject of state scrutiny. There is wide overlap with federal language regarding these same entities.

The major difference between federal regulatory language and that of the states is in the purposes for regulation. While language in both systems covers the goals of (1) maintaining the stability of the banking and financial services industry, (2) providing convenient services, and (3) concern for the public interest in safety and security of deposits and investments, the state statutes have one striking characteristic that differs from the federal. State regulators are specifically charged to promote "economic development," "economic growth," "growth of investment opportunities," or some similarly phrased mission to bring new and expanding business to the subject state.

Jurisdiction

Most state regulatory agencies have authority to examine all depository and non-depository institutions for compliance with both state *and* federal laws. Such authority typically includes state chartered banks, national banks, state savings banks, federal savings banks, branches of out-of-state banks of all kinds, trust companies (special entities established to hold property subject to a trust, to buy and sell securities for others, and to offer advice on these matters), securities and commodities dealers, and building and loan associations. Many states are expanding the authority of their regulators to include entities such as personal loan vendors and makers, personal property finance companies, mortgage brokers, check sales and cashing services, and companies engaged in transportation of money and valuables. All of this latter category of

entities will become very active in the electronic movement of value. This extension and broadening of jurisdiction at the state level is particularly important as the number of multistate holding companies grows.

Techniques of Regulation

Discussions with senior managers in national banks and multistate holding companies indicated that the techniques used by state regulators and the competency of the regulators vary widely. In the past, some states tended toward the strict regulatory paradigm of across-the-board standards, while others tended toward forbearance and mediation of difficulties that a state-charted bank, for example, might be undergoing. This stems, apparently, from the state agency goal of maintaining and encouraging growth and economic activity in the state.

6.3 Regulations and Critical Infrastructure Protection

6.3.1 Impact of Regulations on Critical Infrastructure Protection

In view of the industry's current and future reliance on electronic data transfer, the security of critical infrastructure in banking and financial services is primarily a function of its vulnerability to electronic manipulation or attack. In general, the reality of current practice has outstripped the regulatory system in this area. As one expert in the field put it:

> Without certainty in the legal rules, electronic commerce will not reach its . . . potential . . .Yet the law always lags behind technology.[81]

Banks and other financial institutions, acting in their own self interest, apply various mechanisms and methods to ensure the security of transmitted information. However, these decisions are not generally driven by a need for regulatory compliance. Vulnerabilities and the regulatory situation for major electronic vehicles are summarized below.

Electronic Funds Transfers (EFTs)

This term generally applies to the movement of funds from one bank account to another by means of electronically communicated payment instructions. A major departure from traditional practice is that an EFT for which a bank and its customer have established an authentication protocol is effective as an order of the customer, whether or not it was authorized by the customer, if the bank shows that it fully complied with the agreed-to protocol. According to the banking community, the major threat posed by EFT is from organized crime. The movement of value at light speed makes detecting and tracking money laundering and other illegal practices

[81] Smedinghoff, Thomas J., *Online Law*, Addison-Westley, 1996, p.4.

very difficult. Another threat could come from intentional manipulation of certain markets at levels that are too low to detect, but that yield great profit to the criminal element. If criminal hackers could get into the EFT system and manipulate the apparent market for U.S. Treasury products for half a day, they could "earn" hundreds of millions of dollars from straddles that they created.

EFTs are handled by only a few systems in the United States. These are listed in Table 6.3.

Table 6.3 Electronic Funds Transfer Systems

System	Users	Uses
Automated Clearing House (ACH)	>22,000 financial institutions, >160,000 corporations, and several million private parties	Payment to vendors and suppliers, consumer payments, direct deposits
FedWire	Federal Reserve Banks	Intermediation, settlement, and closure
Clearing House Interbank Payments System (CHIPS)	New York Clearing House Association (12 Money Centers and 125 associate banks)	International funds transfers among members
Society for Worldwide Interbank Financial Telecommunications (SWIFT)	>1,700 banks in >80 countries	Transmittal of payment orders and tenders; settlement is via one of the other systems.

Responsibility for the security of these systems lies with the operators. There is no direct security supervision or regulation by any governmental authority. State statutes and the federal Electronic Fund Transfer Act[82] are directed at consumer protection and elimination of fraudulent practices in electronic commerce, but they do not address system security. Standards and best practices are based on business needs and the result of after-the-fact legal action.

Electronic Checking

As with other forms of electronic commerce, this electronic analogue of paper-based checking relies on use and security of electronic signatures. Protocols for transmission and authentication of these electronic signatures are still under development, and regulation is changing as rapidly as the technology. At present, all states have some kind of legislation that attempts to define what must be protected and what standards of protection should apply. Federal legislation on the same theme is pending. The principal threat is, again, that technology and attendant practice is changing faster than the regulatory environment can be adapted.

[82] 15 U.S.C. § 1693

Digital Cash or Tokens

As described above, this technology is considered vulnerable to misuse for money laundering. There is growing concern about the potential for illegal use of this technology to support the world traffic in illegal drugs. Current proposals center on reporting money movements in excess of $750 to the Internal Revenue Service and analyzing these reports for suspicious patterns.[83] This approach will work only so long as there is some exogenous source of information that will focus the attention of the detection and tracking technology. The cost of any other means to limit the search space would be astronomical.

6.3.2 Measures for Improvement

It is evident that federal and state regulatory practices can have a significant impact on the safety and security of the banking and financial services industry in terms of balancing economic risks and opportunities. It is not at all clear what impact regulation can have on protection of the industry from intentional acts by hostile elements.

Security and safeguard measures taken by this industry have been more directly related to industry concerns for protection of assets than in response to any regulatory pressure. The impact of infrastructure protection is actually felt more directly through regulation of the telecommunications industry than through regulation of banks and financial services firms. That will not be the case in the future.

Historically, major reforms in the regulation of banking and financial services have followed in the wake of crises. That pattern may continue. Alternatively, regulatory systems might be adapted to provide the flexibility necessary to achieve public policy goals, such as infrastructure protection, without unduly compromising the health of the industry. Consideration of the following issues may serve to anticipate problems before they become severe.

1. *Rethinking oversight structure*. The lines between federal and state regulatory practices and structures must become as transparent as the lines between local, state, national, and international commerce in financial products and services are becoming. This will require rethinking the point of balance between supervisory and regulatory approaches to practice, and assignment of oversight responsibility to the level closest to the commerce being conducted. Research is needed on the appropriate regulatory structure for federal and state oversight of the emerging banking and financial services infrastructure.

2. *Development of On-line Techniques for Oversight.* Responses to problems must be much more immediate than has been the practice in the past. Regulators and examiners must begin to monitor the activities of the industry by observing on-line traffic, rather than

[83] "Treasury Seeks Tighter Rules on Wire Transfers," *The Washington Post*, May 20, 1997, Section 1, pg. 1.

depending on periodic reports generated after-the-fact. Research is needed on how federal and state regulators can conduct on-line supervision and oversight. This research should include techniques such as pattern recognition, expert systems, and risk-assessment tools available on-line to both the industry and regulators, so that problems can be quickly identified and acted upon.

3. *Development of On-line Training*. The need for timely and economic training and continuous education for examiners will become greater as changes in the industry broaden and accelerate. The use of the new tools mentioned above and the nature of the emerging and evolving infrastructure that they are intended to address are complex and not familiar to most examiners and regulators. Research is needed to develop distance learning capabilities and on-line expert systems to help prepare and train examiners and regulators.

4. *Development of Standard Definitions of Terms.* The definitions of products, practices, and prices in the industry must be harmonized between state and federal statues and regulations. It must be clear to all concerned what is being regulated when transactions are taking place among billions of actors in cyberspace 24 hours a day. Research and model law development are needed to clarify the subject matter of regulation in the emerging infrastructure and harmonize the laws and regulations among agencies and between levels of government.

[This page intentionally left blank.]

7 TRANSPORTATION INFRASTRUCTURE

7.1 General Description of Regulation

7.1.1 Current Regulatory Environment

The U.S. transportation industry consists of a wide and diverse network of carriers and supporting infrastructure for highway, rail, air, and water transport. Regulation of the industry reflects this diversity. At the federal level, regulatory authority over transportation infrastructure is organized on a modal basis. These modal authorities, now almost exclusively vested within the U.S. Department of Transportation (DOT) are as follows, with some modest overlap:

- Federal Highway Administration (FHWA): highways and bridges (funding for maintenance and replacement; structural and technology research);
- Federal Aviation Administration (FAA): airport and aircraft safety (including navigation facilities for commercial and general aviation);
- Federal Railroad Administration (FRA): railroad safety law administration and enforcement;
- Surface Transportation Board (STB): mergers and infrastructure modifications of commercial carriers;
- Federal Transit Administration (FTA): mass transit (funding for capital investment and operating subsidy, administration and enforcement of federal safety requirements);
- Research and Special Projects Administration (RSPA): safe transport of hazardous materials;
- U.S. Coast Guard (USCG): Administration and enforcement of safety laws pertaining to domestic waterway transport; and
- Maritime Administration: Administration and enforcement of safety laws and multilateral compacts pertaining to international marine commerce using U.S. ports.

Each of these agencies enforces safety and reliability of service through its own regulations. In addition, some of the agencies set priorities for infrastructure maintenance and upgrades by serving as conduits for federal funding.

The mode-based arrangement is generally echoed in the structures of state government transportation agencies, with separate bureaus for roads, railroads, airports and so on. Road

construction and maintenance is generally the largest dollar-volume activity. Many state departments of transportation have regional offices to provide close local supervision of transportation infrastructure.

7.1.2 Current Trends in Regulation

Governmental decisions at both the federal and state levels continue to play an important role in the use and fate of transportation infrastructure. Governmental agencies retain both an outright proprietary interest in certain infrastructures (e.g., highways, seaports and airports) and an indirect interest in others through the direction and administration of funding for infrastructure addition, enhancement, and safety.

With the exception of waterway transport, all modal areas have experienced considerable federal deregulation over the past few decades. The role and presence of governmental regulation in transportation activities has diminished, thanks in part to several (again generally mode-specific) pieces of federal legislation:

- The Airline Deregulation Act of 1978 (Pub. L. 95-504, 92 Stat. 1705, October 24, 1978; codified and subsequently revised in 49 U.S.C. Section VII) removed pricing and service provision requirements for commercial carriers, and opened the market to much easier access by start-up operators.

- The Staggers Rail Act of 1980 (Pub. L. 96-448) basically declassified railroads as fully regulated carriers and empowered them to enter into rate and service contracts with shippers in a manner unconstrained by minimum level-of-service or fixed commodity rate requirements.

- The Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA)(Pub. L. 102-240), declared the Interstate Highway System complete and thereby decentralized much of FHWA's direct authority over highway and bridge project funding.

- The Interstate Commerce Commission Termination Act of 1995 (Pub. L. 104-88), in recognition of the modern success of intermodal freight competition, terminated the ICC. The ICC had been established during the era when railroads were the only source of quick, reliable transport in many areas, to mitigate the excesses of the railroads' monopoly power.

One state-level regulatory area that has shown recent growth is the designation of routes for shipping hazardous materials. States designate particular routes for transport of hazardous cargoes to reduce accident risks, for example limiting them to bypass routes rather than through downtown areas.

In general, far more actual decision-making authority is now vested in private ownership of

transportation facilities than at any time since the late 19th century. However, relationships between the former regulators and those they regulated persist in many manifestations both formal and informal, and to a considerable degree color perceptions on both sides about responsibility for the maintenance of system integrity and security.

7.2 Description of Selected Regulatory Agencies

7.2.1 Selection Method

Good examples of current regulatory relationships and their effects can be found by studying the FHWA, FAA, FRA, STB, and various large-state transportation agencies, among which is the Illinois Department of Transportation (IDOT). A review of the activities of these five agencies and how their regulatory authority affects critical transportation infrastructure is presented below.

7.2.2 Agency Descriptions

7.2.2.1 Federal Aviation Administration

The Federal Aviation Administration (FAA) certifies aircraft and aircraft manufacturing (through issuance of "airworthiness directives"), regulates airport security standards, and is the lead agency for rulemaking on commercial aviation practices. It was established by the Federal Aviation Act of 1958 and is charged with promoting the growth and safety of civil and commercial aviation through constructive regulation and oversight. Today the FAA has a well-publicized role in overseeing airline passenger safety and airport security. It also regulates commercial air freight transport and civil aviation (private aircraft).

In addition to its regulatory role, the FAA owns and is responsible for much of the *in situ* infrastructure that supports air navigation, including control towers and regional control centers, very-high-frequency omni-range (VOR) radio navigation beacons, Doppler radar installations, and visual approach slope indicator (VASI) and instrumented flight rule (IFR) landing lights and structures. Commercial and most civil aviation could not function without these facilities.

7.2.2.2 Federal Highway Administration

The FHWA was created in the 1966 Department of Transportation Act.[84] It is charged with implementing "highway safety programs, research, and development related to highway design, construction and maintenance, traffic control devices, identification and surveillance of accident locations, and highway-related aspects of pedestrian safety."
Despite considerable delegation of authority to states under ISTEA (see above), FHWA retains

[84] *See* 49 U.S.C. §104.

major funding responsibility for capital improvement and augmentation projects on the designated National Highway System (including the Interstates) and provides technical guidance to states on road and bridge construction standards and safety. FHWA maintains the inventory of the over 575,000 bridges and structures on U.S. highways, whether on or off the federal-aid system. Probably FHWA's most important fiscal function is apportioning and distributing the respective states' shares of Congressionally authorized fiscal-year funding for highway projects. However, the FHWA has relatively little discretion in allocating this funding; most is dictated by formulas incorporated into the authorizing statutes.

A second key function of FHWA with regard to the security and integrity of national highway infrastructure is research and development. The FHWA performs research and also sponsors research by other organizations pertaining to materials science. Much of this activity is performed and coordinated through FHWA's Turner-Fairbank Highway Research Center in McLean, Virginia. Ongoing projects related to concrete performance and deterioration modes, advances in structural reinforcement mechanisms, and optimal channeling of traffic flows (leading, for example, to better designs for freeway interchanges) keep Turner-Fairbank prominently involved in road and bridge improvement efforts.[85]

7.2.2.3 Federal Railroad Administration

Safe practices on U.S. railroads are regulated and enforced by the FRA. The FRA was created in the 1966 Department of Transportation Act, and its primary function is spelled out in 49 U.S.C. Section 103: "to carry out all railroad safety laws of the United States . . . [the FRA is] responsible for all acts taken under those laws and for ensuring that the laws are uniformly administered and enforced."

The FRA railroad safety rules are spelled out in 49 CFR Part 209 *et seq*. Track, structures, rolling stock, and locomotives are subject to unannounced inspections. There are also numerous regulations pertaining specifically to rail shipment of hazardous chemicals; the FRA is

[85] A specific example of a project responsive to a potential threat to infrastructure integrity is the ettringite distress program, initiated by the Turner-Fairbank Center in 1996 in response to a request from FHWA Region VI. The Texas department of Transportation had discovered that a calcium aluminum sulfate hydrate material called ettringite had formed (possibly due to unusual water and heat exposure conditions) from the concrete in pre-cast bridge support beams awaiting installation at a highway construction site. Expansion cracks had appeared where the ettringite was forming, and the beams were written off as unusable. Unfortunately, ettringite was later discovered in beams that had already been installed at several other locations around the state. Pursuant to the request of Region VI, Turner-Fairbank's Exploratory Research Team developed chemical thermodynamics models to study ettringite formation, evaluated samples of damaged material, and applied an advanced impact-echo ultrasonic system to evaluate the nature and cause of the microcracking of the concrete. Effort and expertise from the National Institute of Standards and Technology (neutron diffraction instruments) and the University of Hawaii (laser scanning microscopes) were also brought into play. The overall objective was to isolate the exact damage mechanism and the conditions under which the damage occurs, and to evaluate whether concrete specifications for future jobs must be changed to mitigate the threat and if damage to existing structures is repairable in place. (Source: FHWA Web page announcement, 1997).

empowered to levy fines and other penalties on both shippers and carriers for failures in marking and labeling, inspection and handling procedures, crew training, or other requirements.

Under 49 CFR Part 240, FRA also spells out certification requirements for individuals authorized to operate locomotives. Included in these requirements are (1) written evidence of positive prior safety conduct, including operation of a highway motor vehicle (i.e., driving record); (2) no current record of substance abuse; (3) ability to meet specific vision and hearing standards; (4) qualification for road service by means of a written examination covering personal safety practices, operating practices, equipment inspection practices, train handling practices, and compliance with federal safety rules, as well as by means of an operational test at the controls of either an actual locomotive or locomotive simulator; and (5) periodic performance monitoring by qualified supervisory personnel.

7.2.2.4 Surface Transportation Board

The STB, successor to the ICC under Title II, Sec. 201(a) of Pub. L. 104-88 (the ICC Termination Act of 1995), reviews and approves proposed railroad and motor carrier mergers and the resulting trackage rights (authorization to move cargo with its own rolling stock and motive power) that will be granted to competing carriers over certain lines of the merge partners. It also authorizes return to service (following appropriate safety checks) of railroad lines that have been inactive. Its specific mission, as articulated in 49 U.S.C. § 702, is to carry out activities of the ICC "not otherwise abolished." As discussed below, activities meeting this definition are rather limited.

ICC regulation of rail transport was largely concerned with protecting shippers from potential price gouging or service cutbacks by railroads. This led to curtailments on railroad restructurings such as mergers, acquisitions, and line abandonments. It is clear that the STB endorses the notion that, because shippers and carriers are now fully able to negotiate both short- and long-term haulage rates on a one-to-one basis, and the trucking industry is always standing by to offer "just-in-time" service when needed, shippers no longer require protection from predatory pricing or poor service. All they need is the opportunity to negotiate for better terms from other carriers if dissatisfied with the current provider. Thus, much of the U.S. rail network, formerly tightly controlled by owning carriers capable of restricting access by other haulers unless they agreed to often stringent terms, has been thrown wide open to access by multiple providers of rail services. It is not now unusual to see the locomotives of three of more railroad companies pulling trains along the same stretch of railroad line, and while the "guest" carrier must still pay access charges to its "host," it retains far more control, from origin to destination, over its originating commodity shipments than in the ICC days.

7.2.2.5 Illinois Department of Transportation

IDOT, like many of the large-state departments of transportation, retains substantial authority over intrastate road and transit project funding and contracting, airport planning, and railroad crossing protection standards and equipment. IDOT also participates in *inter*state coordination of

infrastructure management (e.g., multistate "smart" highway corridors). IDOT's mission is to provide cost-effective, safe and efficient transportation for the people who live, work, visit and do business in Illinois, and to ensure that the system supports the state's economic growth. The IDOT modal divisions and their respective responsibilities are as follows:

- *Division of Highways*. Directly manages or oversees the design, construction, operation and maintenance of the 17,000-mile state highway system (including the state's federal-aid highways: the Interstates and the Illinois portion of the National Highway System) and administers the state's local roads and streets program. Total road mileage in Illinois is approximately 138,000, making it the third largest system in the nation.

- *Division of Aeronautics*. Works with local airport agencies to maintain and upgrade the state's airport system (at 138 airports, 280 heliports, and nine balloon ports the second largest in the nation), and plans and develops new airport capacity as needed. This division is also responsible for developing aviation safety and education programs and assisting the Civil Air Patrol.

- *Division of Public Transportation*. Provides technical assistance and administers state and federal funding (including capital grants for purchase and upgrading of track) to 50 public transit systems in Illinois, serving about 600 million passenger boardings a year.

- *Bureau of Railroads*. Administers rail service programs that (1) supplement the passenger service provided by Amtrak, and (2) preserve rail freight service critical to keeping and expanding industry and employment in the state. Also coordinates with and may directly participate in the periodic inspections performed by agents of the FRA to determine compliance with railroad safety rules and operating practices.

- *Division of Traffic Safety*. Compiles crash data; evaluates and analyzes information used to identify highway improvement needs in problem areas; enforces and provides education on safety belt and DUI laws; inspects school buses, trucks and ambulances; and oversees the transport of hazardous materials.

Thus, IDOT exercises authority across the entire spectrum of Illinois transportation activities, and is available to consult with shippers, carriers, operators, passengers, and the general public on matters relating to security and safety of transportation properties and physical plant.

Illinois is one of several states that stands to gain a substantial increase in funding authority for transportation projects if Congress directs more federal highway fuel tax revenue back to its originating states. A number of candidate reauthorization bills currently under Congressional scrutiny incorporate this provision. Such a development would be in keeping with the trend to decentralize administrative power in recent years, and would constitute a windfall for IDOT in terms of both resources and influence. Whether a more pronounced regulatory posture for IDOT would also ensue remains open to question.

7.3 Regulations and Critical Infrastructure Protection

5.3.3 Impact of Regulations on Critical Infrastructure Protection

The transportation industry in the United States is well developed, well interconnected, and generally robust. It is a strong and resilient system. In addition, different methods of transportation are fungible to a considerable degree; that is, if one transport system is unavailable, another may be substituted. In short, the potential for major disruption of our ability to move people and goods from one part of the country to another appears relatively small. However, as recent terrorist incidents have shown, there is a potential for loss of life and significant disruptions on a more local scale.

With over 575,000 bridges and 4 million miles of road in the nation's highway system, as well as some 135,000 privately-held railroad miles and about 200 commercial airports (25% of the domestic airport total), continuous security monitoring of all of our transportation infrastructure is a logistical impossibility. The primary — and certainly a very productive — contribution that regulatory bodies make in the area of transportation infrastructure security is promoting a reasonable level of vigilance on the part of the owners and operators of the infrastructure. The regulatory agencies generally have appropriate powers that can be used to achieve this end, as illustrated by the following examples.

Curtailment of Service

Federal and state transportation agencies are generally empowered to curtail service whenever demonstrable threats to public safety exist and are not corrected by the responsible operator. A recent example of this was Emergency Order 19, issued by the FRA in February of 1996, which halted operations of the Tonowanda Island Railroad over a bridge on its property that crossed a navigable waterway (a tributary of the Niagara River). The bridge had repeatedly been cited by FRA inspectors as structurally unsafe. Use of the bridge was halted because of (1) the railroad owner's chronic failure to respond to prior citations, (2) the potential danger posed to recreational boaters on the river, and (3) the danger of violating international pollution accords with Canada in the event that a train should break through the bridge and spill debris and effluent into the waterway. Another, better known, example was the suspension of ValuJet commercial flights (on grounds of not protecting passenger safety) pending the results of the investigation of the 1995 crash near Miami International Airport.

Training directives.

A regulatory agency will sometimes uncover potentially serious gaps in the content of training given to private sector employees charged with vehicle upkeep, passenger and cargo screening, scheduling and logistics of operations, structural maintenance, and the like. Under most circumstances, the agency is then empowered to issue rules about the content of training as well

as certification of those who have completed such training (including on-the-job experience). One example is FAA's advance notice for a proposed rule on uniform certification of airport security company employees.

Structural Inspection and Maintenance Protocols for Public Roads

Preservation of the structural integrity of the public roads system requires a certain amount of uniformity in inspection and maintenance procedures. IDOT is one of many state Departments of Transportation that, together with their contractors, follow a fixed set of procedures for structural inspections and improvement designations. In order to qualify for state and federal-match funding, an upgrading or replacement project must appear on an approved project list, called the one- or five-year Traffic Improvement Program (TIP). An inspection report indicating priority need for repairs is one of the key ways of getting on the TIP list. As a result, roadways are periodically inspected for signs of trouble, particularly at vulnerable points such as bridges.

Airport Security

The FAA has become increasingly concerned about security practices and procedures at airports. In the wake of the crash of TWA Flight 800, scrutiny of the background, credentials, and training of ground airport staff, especially those working in passenger and cargo screening areas, has moved to center stage. In April 1997, the FAA implemented a new rule, applicable to air carriers and airport authorities, designed to increase airport security by controlling information about airport security procedures.[86] Pursuant to 14 CFR Part 108.5, air carriers are responsible for screening passengers, carry-on baggage and checked baggage with approved screening devices; controlling access to aircraft and air carrier facilities; and reporting and responding to bomb threats and hazards discovered during screening. Under the new rule, they are not to disclose information about these functions except on a "need-to-know" basis. Similarly, employees of airport authorities having information about the air operations area (control tower and related command centers) may no longer share this information freely. Specifically, the following types of information are considered "sensitive security information" (SSI):

- The content of any approved or standard security program for an air carrier, airport operator, foreign air carrier, or the air transport of United States mail;
- The content of FAA Security Directives and Information Circulars;
- The description of screening profiles used for persons, baggage, or cargo;
- The implementing guidance or other information, comment, or instructions pertaining to a security contingency plan;

[86] See 62 FR 13736, March 21, 1997, rule amending 14 CFR Parts 107, 108, 109, 129, and 191.

- The technical specifications of any device used to detect weapons, explosives, or destructive substances; the descriptions and specifications of objects used to test screening equipment; and the technical specifications of security communications equipment;

- Information that would reveal a potential systematic vulnerability to attack of the aviation system or facilities (such as a specific location where a security violation occurred);

- Information about threats against civil aviation;

- Information about assignments and logistics of Federal Air Marshals; and

- The content of proposed changes to security procedures, information, or records.

FAA is also proposing a rule (Docket No. 28859, posted March 11, 1997) that would strengthen requirements for background checks on the employment and criminal history of those who perform checkpoint screening functions at airports. These procedures would now include fingerprint checks for those holding unescorted access privileges to airport security areas. It is believed these additional safeguards have been rendered necessary by the proliferation of contract screening companies, whose employees are not under direct control of the air carriers or airport authorities. The air carrier(s) for whom the screening is being conducted would have the responsibility to assure that the background checks are performed.

The FAA, in an Advanced Notice of Proposed Rulemaking issued March 11, 1997, is also seeking to establish a uniform certification protocol for airport checkpoint security screening companies in order to assure full compliance with the Air Carrier Standard Security Program set forth in 49 CFR Part 108. At the moment, the Agency is only soliciting comments on how this should be done.

5.3.4 Measures for Improvement

A survey of transportation regulatory arrangements reveals a number of areas where regulatory adjustments might be appropriate in the name of increased infrastructure security. In addition, there is one newly emerging practice — centralized traffic management in urban areas — that may lead to a new set of vulnerabilities. There is the opportunity now to incorporate security concerns into the development stage of this technology. Detailed below are the current and future issues identified for enhancement of transportation infrastructure security.

1. *Airport security*. As described above, the FAA is in the process of implementing new rules to increase security at airports. The now-final rule, restricting information about airport security procedures, will presumably make it more difficult for terrorists to circumvent security. However, it is also important that the rule be interpreted and

applied in such a way that it does not stifle debate regarding the efficacy of current procedures. For example, the television show *60 Minutes* recently highlighted alleged shortcomings in airport security. Public discussion of such issues may lead to the sort of scrutiny and pressure that uncovers problems and makes resources available to solve them.

The proposed rule on background checks for security personnel is aimed at maintaining the effectiveness of passenger and baggage screening procedures. The growing use of independent contractors to perform these functions has complicated the process of maintaining security requirements; an insufficiently trained or conspiratorial employee might allow a harmful device to pass. Implementation of the proposed rule has the potential to reduce this possibility.

2. *Protection of aviation control hardware*. As noted in section 7.2.2.1 above, the FAA owns and is responsible for much of the infrastructure that supports air navigation, including airport control towers, landing lights and other structures, plus regional control centers, VOR radio navigation beacons and Doppler radar installations. This physical infrastructure is essential for air navigation and damage to it could shut down an airport. Some of the key items are within the perimeter of airport security, but others, especially the regional control centers and VOR beacons, are located at either decentralized or remote rural sites with little or no active security present. A review of security requirements for these facilities should be considered.

3. *Protection of key rail facilities*. The Arizona Amtrak derailment in 1995 indicated the potential for terrorist attack directed at rail infrastructure. The track was damaged sufficiently to cause a derailment, and the damage went undetected because the perpetrators tampered with the electronic track monitoring system. FRA standards cover electronic railway track communications and signaling system standards but do not provide for controlling or mitigating *override* of these systems by unauthorized intervention. Clearly, most rail carriers want to have appropriate security and inspection measures in place on their major lines, but resource constraints may preclude such provision on secondary lines (as in the Arizona case) unless a specific regulation were to require it.

   Another issue relating to key rail facilities is the presence of a relatively small number of "choke points" in the rail network that connects the eastern and western U.S. There are six locations (mostly major rail junctions) where east-to-west rail lines converge; simultaneous disruption at those six points would sever all U.S. rail connection between the coasts.[87] These six rail funnel points may deserve consideration for upgraded security in the national interest.

[87] It should be noted, however, that traffic could still be rerouted through Canada, unless rail tracks there were also attacked. In addition, highway truck transport could be substituted for most commodities.

4. *Protection of rail passenger terminals*. In some locations, rail passenger facilities are located with or nearby freight facilities. This configuration represents a vulnerability in that hazardous materials or explosives could thus be brought into proximity with a crowded area. No regulation requires complete (lateral) physical segregation of freight cars from passenger equipment in use; a regulation that stipulates internal inspection and locking of freight cars prior to their storage on tracks near rail passenger loading facilities may merit study.

5. *Highway funding formulas and FHWA discretion*. Under various sections of Title 23 of the U.S. Code, FHWA is given a degree of license in including demonstrated need as a criterion in computing funding allocations to states (although admittedly the final allocation remains based on established formulas). However, it is not specifically within FHWA's purview to attach, as appropriate, an *infrastructural security or safety* dimension to the concept of need. Any proposed infrastructure improvements of a capital nature might require legislative adjustments to allow use of security considerations in determining funding.

6. *Security of advanced traffic management systems*. Plans are being developed to establish advanced traffic-management systems to relieve congestion on urban roadways. At such facilities, personnel will monitor roadway conditions in real time and implement (or monitor) computer-controlled modification of intersection and freeway access ramp signal timings and variable message signs (hazard warnings, potential reroute guidance). Such systems have the potential to make traffic flow more smoothly — or, if misused, to tie it up, impeding passage of emergency vehicles as well as ordinary traffic. Efforts are already underway to privatize the operation of the these new traffic management centers: while the roadway system itself remains under public jurisdiction, private entities will in many cases be contracted to operate the facilities. State departments of transportation and local authorities will oversee these privatized installations in terms of contractual compliance. Study of methods to include security measures in the oversight agenda may be appropriate.

[This page intentionally left blank]

8 DRINKING WATER INFRASTRUCTURE

8.1 General Description of Regulation

8.1.1 Current Regulatory Environment

Most drinking water is supplied to the public by municipal water systems. There are also private systems for subdivisions or large commercial or governmental facilities. A water system consists of a water supply (either groundwater wells or surface water), a treatment facility, treated water storage facilities, and a distribution system. The configuration of a water system varies depending on the source of water, type of treatment applied, and number of connections to be served. Smaller systems may have minimal treatment facilities in each well house, while larger systems may have a centralized treatment facility. Small systems can distribute the water directly from the source or treatment facility, while larger systems require treated water storage facilities to meet peak demand and maintain system pressure. Some systems consist only of distribution lines and purchase their water from another water system. In general, these municipal distribution systems are exempt from regulation other than local interior or connection plumbing requirements.

The regulation of drinking water systems is conducted primarily by state agencies, but according to federally established standards. The Safe Drinking Water Act (SDWA) (Public Health Service Act, 42 U.S.C.A. §§ 300f to 300j-26) authorizes the U.S. Environmental Protection Agency (EPA) to promulgate regulations applicable to water supply systems; perform studies on drinking water sources, technologies, and health risks; and assist states in implementing drinking water programs. In general, the EPA drinking water regulations address water quality standards, treatment methods, system operations (i.e., system water pressure, operator certification, and engineering requirements), and construction standards. EPA also protects drinking water sources via its underground injection control program, watershed demonstration program, sole source aquifer protection program, and wellhead protection program. These latter regulations, however, are not directly applicable to drinking water suppliers but are instead concerned with identifying potential sources of contamination (landfills, surface impoundments, underground storage tanks of special waste, the application of pesticides and fertilizers, etc.) near public drinking water sources or over areas that recharge drinking water sources.

The EPA Office of Ground Water and Drinking Water directs the National Drinking Water Program, including the establishment of drinking water maximum contaminant standards, monitoring requirements and techniques, and groundwater protection programs. All state programs must adopt regulations at least as stringent as those promulgated by the EPA. If a state does not have an EPA-approved drinking water program, the EPA itself implements and enforces the SDWA in that state. States may also enforce their own additional regulations to address economic matters (such as rates and access to public rights of way), or local hydrological conditions. Generally the SDWA standards are enforced by the state environmental protection agency. Other regulations, such as those for rate approval, may be performed by a state public

utilities commission (PUC) or similar body. In any state that has not applied for and obtained approval of an enforcement program, or whenever the EPA Administrator finds an authorized state is not duly enforcing the national primary drinking water standards, the EPA Administrator may take enforcement actions.[88]

Local plumbing ordinances are enforced by municipalities or counties. These ordinances pertain to plumbing inside buildings and the connections to any public water system but not to the operation or construction of the public water system itself. Plumbing ordinances are enforceable against anyone constructing or modifying a building within the municipality's or county's jurisdiction. Often, if the municipality or county is also the owner/operator of the public water supply system, it is required to promulgate and implement such local plumbing regulations and standards to comply with state water supplier laws and regulations. Non-municipal water companies, which must comply with the state water suppliers regulations but do not have legal authority to promulgate their own ordinances, can still require any applicant for water service to comply with their plumbing and connection requirements and standards.

Usually these plumbing regulations are designed for the protection of the water system from improper piping systems and illegal connections to the potable water supply. They may include requirements for (1) installing backflow prevention devices for certain kinds of equipment and appliances, (2) using particular materials for building internal piping systems (e.g., no lead pipe or soldering or PVC piping), (3) providing venting, and (4) applying to connect to the public water service main.

8.1.2 Current Trends in Regulation

The SDWA was amended in 1996, but there has been no trend toward significant deregulation and no shift in regulatory jurisdiction as a result. The amendments eliminate the automatic requirement that the EPA list additional contaminants for monitoring and treatment every three years. The updated process for setting drinking water standards focuses on contaminants known to pose greater health risks (such as *Cryptosporidium).* The amendments require a new regulation for radon in drinking water and studies of the health effects of sulfate and arsenic in drinking water. The amendments also allow for limited alternatives to current filtration and groundwater disinfection regulations. Other provisions focus on assurance that water supply companies can provide sufficient capacity to meet future needs and on the ability of small water companies to meet the current regulations.

Some of the provisions in the 1996 amendments may affect the security of the drinking water infrastructure. These are discussed below.

[88] In these cases, the EPA may issue administrative orders against any water company not in compliance with the national primary drinking water standards and may enforce those orders in the federal district court.

The disinfectants and disinfection by-product rule was first proposed in July 1994. It is currently in the negotiated rulemaking process. Public water systems use disinfectants to kill harmful microbial contaminants. However, disinfectants and their by-products may also pose risks, including potential increases in rates of cancer, liver damage, and kidney damage. In Stage I, the standard for certain disinfectant by-products (e.g., trihalomethanes) would be lowered. However, any rule to control these disinfectant by-product health risks must also consider maintaining a level of disinfectant that will protect the population against microbial risk. There is currently a regulatory requirement to maintain a specified level of chlorine residual in all parts of the distribution system. This requirement is intended to eliminate chlorine-sensitive contaminants that may be introduced into the water distribution system. However, if the new rulemaking lowers the level of chlorine residual, although the disinfectant level may be considered safe for normal microbial risk, it may no longer protect against the introduction of a more potent microbial agent.

Although many authorized state programs already include water plant operator certification requirements, the amendments require EPA to promulgate operator certification guidelines that must be adopted by authorized states or the states will lose a portion of their State Revolving Fund allocations.[89] There is no indication what types of certification requirements are being considered.

The amendments also give a public water system a shorter time to notify its customers of violations of SDWA requirements. Currently, the SDWA mandates that a notice of a violation of a maximum contaminant level (MCL) or of any other violation designated by the EPA as posing a serious potential health effect must be given as soon as possible, but in no case later than 14 days after the violation. The EPA regulations, which are generally adopted by the states, mandate that when a water supplier has exceeded the MCLs of contaminants that may pose an acute risk to human health, it must furnish a copy of the notice to the radio and television stations serving the area as soon as possible, but in no case later than 72 hours after the violation (40 CFR 141.32(a)(1)(iii)). The amendments shorten this time period to 24 hours when there is potential for serious adverse health effects from short-term exposure. It is up to the state implementing agency to determine the form, content, and manner (e.g., broadcast media, newspaper, or door-to-door) of the notice.

The amendments also require states with primary enforcement responsibility to conduct an assessment, coordinated with existing information and programs, to determine the vulnerability of sources of drinking water within the state's boundaries. By August 1997, the EPA will issue guidance for these state source water assessment programs to ensure that they will delineate protection areas and assess contamination risks to source waters. The vulnerability discussed in these programs is the susceptibility of a water source to contamination from either industrial activities or natural conditions. The amendments provide for loans to public water systems to acquire land or conservation easements for source water protection. New subsection 1428(l)(5)

[89] The EPA maintains the State Revolving Loan Fund, which provides funds to state agencies to be used for making loans or loan guarantees to water systems to facilitate compliance with applicable drinking water regulations.

of the SDWA requires the EPA to conduct a demonstration program on the most effective means of assessing and protecting source waters serving large metropolitan areas. However, this program is aimed at protecting water sources from the effects of development and industrial activities rather than intentional contamination.

The EPA has also proposed a Chemical Monitoring Reform Program that would allow states to target systems at risk of contamination for increased monitoring and reduce the sampling requirements for systems not at risk. This program would focus available public resources on the highest priority water systems. Although reduced monitoring may affect the ability of a water system to detect the introduction of a contaminant into the system, contaminant monitoring required by current regulations is not designed to detect intentional contamination, and increased monitoring would not be an effective method of deterring or detecting intentional contamination. (See discussion in Section 8.3.)

8.2 Description of Selected Regulatory Agencies

8.2.1 Selection Method

The following agencies were selected for detailed discussion: the EPA, Illinois Environmental Protection Agency (IEPA), Illinois Commerce Commission (ICC) and the City of Chicago. The EPA was selected because it is the paramount authority on the regulation of public drinking water under the SDWA.

In general, most state programs follow the EPA program closely with few significant state-specific requirements. Illinois is a representative state, and the IEPA and ICC together regulate drinking water supply systems in the state. The IEPA has primary enforcement responsibility for public water systems in Illinois. Its regulations incorporate the federal drinking water regulations, as required by the SDWA, and add a few Illinois-specific regulations. Non-municipal water supply systems in Illinois are regulated as public utilities by the ICC. ICC authority focuses on reliability of service and rates setting.

The City of Chicago Public Works, Department of Water, maintains the public water system for all citizens within the Chicago city limits. It is the largest public water system regulated by the IEPA. It is representative of a large urban system, which is assumed to be a more likely target of terrorist activity. The City of Chicago promulgates its own plumbing ordinances regulating interior building piping and customer hook-up to the potable water system.

8.2.2 Agency Descriptions

8.2.2.1 Environmental Protection Agency

The SDWA (42 U.S.C.A. §§ 300f to 300j-26) authorizes the EPA to establish national drinking water regulations applicable to all public water systems.[90] The SDWA applies to all public water systems in each state.[91] Primary enforcement of these drinking water regulations, however, is delegated to states that have approved drinking water programs. To obtain approval, the state must adopt drinking water standards at least as stringent as the federal (EPA) standards (40 CFR 141) The EPA directly regulates drinking water systems in states that do not have approved state programs or where state enforcement has broken down.[92]

The EPA also has the following authorities and functions under the SDWA:

- Establishes the types and extents of variances and exemptions to national drinking water regulations that can be obtained. Such limitations must be adopted by states with approved programs.

- Establishes the regulations and approves state programs for underground injection control and wellhead protection programs.

- Conducts research, studies, and demonstrations related to (1) the causes, diagnosis, treatment, control, and prevention of physical and mental disease, or (2) the provision of a dependably safe supply of drinking water.

- Provides technical assistance to the states and municipalities to establish and administer public water system supervision programs. The EPA may also make monetary grants to states with approved primary enforcement responsibility to carry out public water system supervision programs and underground water source protection programs.

---

[90] Under EPA regulations, a public water system is a system for the provision to the public of piped water for human consumption, which has at least 15 service connections or regularly services an average of at least 25 individuals daily at least 60 days out of the year. The term includes (1) any collection, treatment, storage, and distribution facilities under the control of the operator of such system and used primarily in connection with such system and (2) any collection or pretreatment storage facilities not under such control which are used primarily in connection with such system.

[91] The act does not cover water systems that (1) consist only of distribution and storage facilities (and not collection and treatment facilities); (2) obtain all of their water from, but are not owned or operated by, a public water system to which the regulations apply; and (3) do not sell water to any person. This exclusion is often pertinent to federal facilities which supply municipal water to their employees and residents without charge through their own distribution systems.

[92] Currently, only Wyoming and the District of Columbia do not have SDWA primary enforcement responsibility. Therefore, the EPA is the enforcement agency in those two states.

- Provides technical assistance and monetary grants to states or publicly owned water systems to assist in responding to and alleviating any emergency situation affecting public water systems that the EPA determines present substantial danger to the public health.

- Is authorized to take action if it receives information indicating that a contaminant may present an imminent and substantial endangerment to public health, and that state or local authorities have not taken appropriate protective action.

- Has primary enforcement responsibility for bringing actions against those who tamper with public water systems.

The SDWA establishes criminal and civil penalties for tampering with public water systems (42 U.S.C.A. § 300i-1). "Tampering" includes the introduction of a contaminant into a public water system with the intention of harming persons or otherwise interfering with the operation of a public water system with the intention of harming persons. Sanctions include imprisonment for up to five years and fines of up to $50,000. Attempting to tamper and threatening to tamper are also subject to (somewhat lesser) criminal and civil penalties.

8.2.2.2 Illinois Environmental Protection Agency/Illinois Pollution Control Board

Under the Illinois Environmental Protection Act (415 ILCS 5/1 *et seq.*), drinking water supplies are regulated by the Illinois Pollution Control Board (IPCB or Board) and the IEPA.[93] The Board issues standard-setting regulations, including those mandated by the SDWA. The Board also conducts hearings upon complaints charging violations of the regulations and determines sanctions. The IEPA conducts the associated administrative functions such as issuing permits, conducting inspections, and sending notices of violation. The IEPA also supervises the state wellhead protection program. The IEPA promulgates its own regulations, setting out how it conducts those duties. Below are summaries of Board and EPA regulations governing various aspects of water supply regulation and enforcement.

<u>Investigation and Enforcement</u>

The IEPA may investigate any drinking water supplier upon the request of the Board or upon receipt of information concerning an alleged violation. The IEPA can then issue a written notice of noncompliance and a formal complaint against the regulated water supplier. The public water system would have to answer the complaint before the Board. In addition, third parties may bring a complaint against any public water system alleging violation of the act or a permit or rule

[93] The IEPA and Board regulations apply to all public water supplies except for those designated as noncommunity water supplies. A noncommunity water supply is one which serves or is intended to serve fewer than 15 service connections used by residents or regularly serves fewer than 25 residents. These small, noncommunity water systems are regulated by the Illinois Department of Public Health under its own regulations (77 Illinois Administrative Code 900 *et seq.*).

issued under it. After the hearing, the Board issues an administrative order that may (1) direct the public water system to cease and desist from violating the Act, rule or permit condition; (2) revoke the system's permit; or (3) impose civil penalties. All such orders are enforceable by injunction, mandamus, or other appropriate remedy in the appropriate state court.

Emergency Authority

When an episode or emergency condition exists, the IEPA so declares, and if the emergency condition creates an immediate danger to health, the IEPA can seal any equipment, vehicle, vessel, aircraft, or other facility operated in violation of regulations or contributing to the condition.

Compliance Monitoring.

State regulations specify the frequency and method of sampling drinking water for each of the drinking water primary and secondary standards; they even designate from which taps samples are to be taken. The supplier must file monthly monitoring reports with the IEPA as demonstration of compliance with the MCLs for the listed contaminants. If the supplier has exceeded any MCL for that month or failed to perform the required monitoring, it must notify the IEPA and make public notice to all its customers in a local newspaper or other form of written announcement.

Construction Standards for New Systems.

Under EPA regulations, a state must have a program that assures that the design and construction of new or substantially modified public water system facilities will be capable of complying with all state primary drinking water regulations. This program ensures that the state enforcement agency maintains up-to-date records of the structure of each drinking water system under its jurisdiction. Also, the state must demonstrate that it has a program that includes maintenance of an inventory of all public water systems in the state. Therefore, the state enforcement agency will have a working knowledge of all drinking water systems in the state, including the structure of their production, treatment, and distribution systems.

The Illinois Act requires all owners of public water supplies to submit plans and specifications to the IEPA and obtain written approval before constructing, adding to, or changing any public water supply installation. The IEPA has adopted very specific regulations governing such permitting and the design and construction of public water systems. The regulations for issuance of a construction permit also require the construction be in accordance with the American Water Works Association Standards (Standards) and the Recommended Standards for Water Works — Policies for the Review and Approval of Plans and Specifications for Public Water Supplies of the Committee of the Great Lakes-Upper Mississippi River Board of State Public Health and Environmental Managers (Recommended Standards). The Recommended Standards are used by

regulators in Illinois, Indiana, Iowa, Michigan, Minnesota, Missouri, New York, Ohio, Ontario, Pennsylvania, and Wisconsin to draft and grant permits for the construction of public water systems.

8.2.2.3 Illinois Commerce Commission

In addition to the Board and IEPA, water utilities operating in Illinois are also subject to regulation by the ICC. The general powers and authorities of the Commission are set out in Section 3.2.2.4 above. Water utilities must obtain certificates of public convenience and necessity and meet all Commission requirements for service and information filings. The Commission also has jurisdiction over the rates and charges of water utilities.

8.2.2.4 City of Chicago

The City of Chicago is a public water system regulated under the IEPA jurisdiction. It operates its system in compliance with those Illinois laws, regulations, and standards. The City Council has also issued ordinances concerning the standards for plumbing within buildings and requirements for connecting to the City of Chicago public water system (Chicago Municipal Code § 11-8-010 *et seq.*). Under these local ordinances, the Chicago Department of Water has free entry and access to every part of any building, structure, or premises and the authority to inspect the plumbing.

Permits must be obtained for the installation of any piping in any building that receives its service from the Chicago Waterworks System. Permits must also be obtained from the Department of Water to open any paved street for the purpose of tapping mains or laying service pipe. Department of Water approval is necessary before a service pipe can be connected to any water supply pipe that is part of the Chicago Waterworks System.

8.3 Regulations and Critical Infrastructure Protection

8.3.1 Impact of Regulations on Critical Infrastructure Protection

The current regulatory regime for water supplies is not specifically designed to prevent hostile acts. The EPA's regulations do not contain any clear, direct requirements for security systems or restricted access to any parts of the water supply system. Nonetheless, the regulations do have a number of features that affect the vulnerability of supply systems to attack. Several such features are discussed below. To put this discussion in perspective, a brief analysis of potential threats follows.

Threat Analysis

Water supply systems may be vulnerable to criminal tampering at any point in the system: water sources (surface or groundwater), production facilities (well or intake), treatment facilities (plant or well house), storage facilities (raw water reservoirs, and treated water tanks or towers), and distribution systems (mains, lift stations, sampling points, and customer connections). Tampering could include introducing a contaminant into the drinking water supply, thereby causing illness or death in the population served by the system, or physical destruction of water system facilities.

Destroying a retaining dam in a supply reservoir would cause a physical threat to those located downstream and could affect water pressure and the amount of water available. Taking out a treatment facility or cutting off service from the water source to the treatment facility could result in the loss of treated, safe drinking water to the public. The loss of potable water would cause an emergency situation; however, it would be clearly evident and could be dealt with (e.g., by issuing boil orders and securing alternative water supplies).

Contamination of a large urban drinking water system is a logistically difficult proposition. As discussed in two reports prepared for the President's Commission on Critical Infrastructure Protection (PCCIP), *Identification and mitigation of Threats to Critical Infrastructures in the U.S. Water Supply System*, June 1997, and *New York City's Emergency Services Infrastructure*, May 1997, dilution effects are so extensive in raw water sources (groundwater aquifers, lakes, rivers, or retention reservoirs) that huge amounts of contaminant would be needed for harmful level to be reached at the tap. Introduction of a contaminant near the inlet of a treatment plant would reduce the amount of contaminant needed; however, subsequent treatment would destroy or remove at least some portion of the contaminant, thus rendering it less effective. Therefore, the following discussion focuses on the deliberate contamination of a drinking water supply at a point after the treatment plant or well house.

Engineering Requirements

EPA regulations require each state drinking water program to establish some method of assuring that the design and construction of new or substantially modified public water system facilities will be capable of compliance with the state primary drinking water regulations. The IEPA has adopted regulations that require the construction of drinking water systems to comply with the AWWA Standards and the Recommended Standards. Most states have adopted one or both of these sets of standards.

These construction standards require certain protection against contingencies: (1) physical protection of source areas, reservoirs and equipment against contamination or tampering and (2) in some cases, provision against possible loss of power or malfunction of treatment equipment. Well sites must be protected from potential sources of contamination through ownership, zoning, easements, leasing or, if required by the IEPA, fencing. Pumping stations must also be access-protected to prevent vandalism and entrance by animals or unauthorized persons. In addition, storage structures for treated water must be protected with fencing, locks, and other necessary

precautions to prevent trespassing, vandalism, and sabotage. The Standards also require that any test wells or other drinking water wells not in use must be sealed to prevent contamination of the water source, preferably by filling the well with cement grout.

There must be provision for standby or backup power in facilities where power outages may result in pressure loss in the distribution system. Standby chlorination equipment of sufficient capacity to replace the largest unit in the supplier's treatment system is also required. In addition, where automated equipment is to be used, supporting data that (1) justify the equipment, (2) demonstrate proper maintenance of the equipment is within the capability of the plant manager, and (3) assure the existence of manual override and manual restart options must be supplied.

Applicants for a permit to build or substantially modify a water facility must submit design information sufficient to show that the finished facility will meet the AWWA Standards and the Recommended Standards. Older facilities are not subject to these requirements, unless or until a substantial overhaul is made.

Maintenance of Plans and Diagrams

The ICC requires each utility to maintain reasonably accurate, up-to-date supply diagrams and distribution maps showing equipment, capacities, and flow directions, including the locations of all mains, hydrants, and valves. The ICC reasons that these maps are necessary to enable the utility to promptly and accurately advise interested individuals on the location of mains and service lines. In the City of Chicago, applications for the installation of piping within buildings and for connection to the potable water system must include plans that clearly show the complete water supply system from the City service to the plumbing fixtures and other appliances, including fire protection equipment. This permitting requirement provides the City with detailed plans of internal plumbing.

Having complete, centralized information of this sort can affect infrastructure vulnerability in two conflicting ways. The general availability of this information may allow terrorists to easily obtain a working knowledge of the water supply distribution system and thereby determine the optimal point for introducing a contaminant or sabotaging critical treatment equipment. However, the information may also be essential for performing quick hazard analyses, repairs, isolation, or other actions in response to an act or threat.

Powers of Inspection

The IEPA and ICC have authority to enter and inspect any regulated drinking water supplier. In addition, the City of Chicago has authority to enter upon the premises and inspect the interior plumbing and any water connections. This authority to inspect might be valuable in preventing the intentional introduction of contaminants, if authorities have information on a possible threat. However, criminal investigation procedures would probably take precedence over civil

inspection procedures in any such instance.

Cross Connections

Cross-connections are any physical connections or arrangements between two otherwise separate piping systems — one that contains potable water, and the other that contains water of unknown or questionable safety, steam, gases, or chemicals — whereby there may be a flow from one system to the other. Direct cross-connections are formed when a water system is physically joined to a source of unknown or unsafe substances. Indirect cross-connections are formed when an unknown substance can be forced, drawn by vacuum, or otherwise introduced into a safe water system.

The Board has issued regulations prohibiting such cross-connections unless there is a physical barrier preventing contamination of the potable water supply. These regulations were promulgated to protect the water supply from the unintentional introduction of industrial chemicals, pesticides, and nonpotable water at specific sites assessed by the IEPA for vulnerability (chemical processing tanks, fire hydrants, laboratory sinks, etc.).

Generally, where such connections exist, a backflow prevention device is installed. It provides a mechanical or air-gap separation between the two systems that prevents the back siphoning of untreated or contaminated water into the water supply system. Each supplier must conduct a cross-connection control survey of the distribution system every two years and must have an ordinance, tariff, or required condition for service that includes a plumbing code at least as stringent as the Illinois Plumbing Code (77 IAC 890). The City of Chicago, as a regulated water supply system, has issued plumbing ordinances to enforce this prohibition against cross-connections.

The impact of these regulations on water system security is that they prevent a situation in which water supplies can be easily contaminated, for example, by turning some valve in an industrial facility.

Operator Certification

EPA and IEPA regulations currently require water plant operating personnel to be certified. A personal interview is conducted; however, the subject is limited to the applicant's familiarity with Illinois requirements and general operating knowledge. Certification does not require a background check or other security investigation. Currently, under the SDWA Amendments of 1996, the EPA is to work with states, public water systems, and the public to develop additional recommended operator certification requirements.

Water Sampling and Monitoring

Water system operators are required to test their water periodically for the presence of certain

contaminants. The types of contaminants and frequency of testing may vary depending on the size of the water system and other local circumstances. The list of contaminants that must be monitored is limited and focuses on the most common sanitary, industrial, and agricultural pollutant hazards. It appears unlikely that current monitoring practices would detect the presence of a contaminant deliberately introduced for hostile reasons. However, the requirements do establish a "monitoring infrastructure" of trained personnel and procedures that might be adapted to perform other types of monitoring as needed.

Water Treatment

Drinking water is generally treated by chlorination and other means in order to eliminate contaminants. This treatment effectively reduces biohazards. Board and IEPA regulations require chlorination be maintained at levels sufficient to provide adequate protection of human health. In addition, the regulations require that water suppliers maintain an active residual disinfectant concentration (RDC).[94] This requirement to maintain a particular RDC throughout the system at all times will continue to protect the water supply from the introduction of chlorine-sensitive contaminants at any point after the treatment plant. However, the level of disinfectant is currently under review in the proposed disinfectant/disinfectant by-product regulation. As stated above, if the new rulemaking lowers the level of chlorine residual that must be maintained in the water distribution system, although the level may be considered safe for normal microbial risk, it may no longer protect against the introduction of a more potent microbial agent.

Emergency Measures

As required by EPA regulations, the Board has adopted regulations concerning emergency operations. Whenever contamination is determined to persist in a public water supply, the owners of the supply must notify all consumers to boil all water used for drinking or culinary purposes until it is demonstrated that the water is safe for domestic use or appropriate corrective action approved by the IEPA has been taken. If the owner fails to take such action, the IEPA may issue a boil order directly to the consumers affected. Any emergency that results in water pressures falling below 20 pounds per square inch (psi) on any portion of the distribution system shall also be reason for immediate issuance of a boil order. Whenever the safety of a supply is endangered for any reason, the IEPA must notify the owner, and the supply system officials must take appropriate action to protect the supply.

City of Chicago ordinances provide that whenever the commissioner of water finds a continuous supply of water is indispensable in any building, structure or premises, the owner or occupant shall provide for a tank or other receptacle of sufficient capacity or for installation of redundant

[94] Residual disinfection concentration is the concentration of disinfectant (free or combined chlorine) measured in mg/L in a representative sample of water.

plumbing with an emergency connection of a second service pipe from an independent source. This authority could be useful for ensuring that critical emergency service facilities (e.g., hospitals, police stations, and designated shelters) have a second source of drinking water during emergency situations.

Source Protection

The EPA's water source protection programs (i.e., underground injection control program, sole source aquifer protection program, wellhead protection program, and watershed demonstration program) are not designed to protect a water source from the intentional introduction of contaminants. They are designed to increase awareness of activities that can, through mismanagement, result in the contamination of an underground water source through migration of surface contamination or through direct well injection into the aquifer. As discussed, however, the intentional introduction of a contaminant into a raw water source is probably not a logical avenue for terrorist activity, since the contaminant would be subjected to dilution and chemical treatment.

8.3.2 Measures for Improvement

Even though current drinking water regulations were not designed to prevent the intentional sabotage of drinking water supplies, they are generally consistent with the protection of the public drinking water supply. The following suggested measures for improvement have taken into consideration the existing regulatory scheme, along with the physical characteristics and operating requirements of a drinking water supply system.

1. *Access restrictions*. It would be impossible to physically protect all the water mains that serve a large metropolitan water system. The City of Chicago Waterworks system has 4,234 miles of water main and serves the City and 118 suburban communities. Similarly, any large metropolitan water system serves millions of residential, commercial, and industrial buildings and has thousands of outside connections such as sprinkler systems, fire hydrants, and water fountains. It would be impossible to adequately secure every service connection to a water main to prevent the intentional introduction of a contaminant. Therefore, to attempt to introduce regulations requiring some kind of physical protection of the entire distribution system would be futile and financially prohibitive.

   It may be worthwhile, however, to identify key points in the system that are likely potential targets and consider additional (or more uniform) requirements for security at those points. In most systems, much of the piping is buried deep underground and relatively difficult to reach. Key aboveground facilities could probably be fairly easily identified and prioritized for protection.

   EPA regulations, as adopted by most states, do not contain any requirements for

restricting access to water production or treatment facilities. A common theme in the drinking water regulatory scheme is the certification or permitting of each water supply system by the state agency and the requirement that the construction of water production and treatment facilities meet certain engineering standards. As discussed, most states have adopted some sort of standards that require the physical protection of water production facilities (locked well houses, fenced pumping stations, etc.) and water treatment facilities. However, there is no uniform regulatory scheme for ensuring physical protection of these critical facilities. It may be possible to work with the existing engineering requirements (e.g., the AWWA Standards or Recommended Standards) to introduce additional security features in construction permits that would provide a measure of protection without imposing financial or operational hardships. Another area to consider for action would be setting minimum security requirements for retrofitting older facilities. Many older facilities already have security provisions such as locks and fences around critical facilities to ensure public safety and to prevent vandalism.

2. *Changes to monitoring and treatment standards*. Monitoring drinking water for contaminants is the primary focus of current drinking water regulations. Currently, all water companies must monitor for contaminants for which MCLs have been established as well as for a list of "unregulated" contaminants. These monitoring requirements are very specific. Monitoring must be conducted by trained individuals, and samples must be analyzed by certificated laboratory personnel. This is an expensive process. Any additional contaminant testing might place a substantial financial burden on water suppliers. In addition, publication of these additional requirements would notify any hostile elments about which contaminants would most likely be detected. Nonetheless, it might be worthwhile to conduct research to identify test methods for detecting contaminants considered likely candidates for terrorist use. Even if not done routinely, such tests could be used following a threat or during periods of heightened security.

   It also might be worthwhile to conduct research on the vulnerability of potential contaminants to existing water treatment technologies. Modest changes in treatment might provide additional protection against such contaminants. Again, techniques might be developed for use on a contingency basis if there is reason to suspect a potential for terrorist activity.

   Another issue in this vein is the effect of the proposed changes in residual disinfectant requirements. It may be advisable for the EPA to consider intentional contamination scenarios in developing and implementing the disinfectant and disinfectant by-product rulemaking.

3. *Information restrictions*. Current regulations require that drinking water system information, including maps, diagrams, and construction details, be available to the public. Such information might be valuable to those planning to attack the system, and so restricting this information might provide a measure of protection. However, there are strong practical reasons why the information should not be restricted. Contractors of all types (e.g., road and building construction, utility construction, and plumbing installation)

need this information to safely conduct their business without harming the water supply system. Instituting secrecy as to the configuration of the system might result in more damage and interruptions of service than terrorists are likely to cause.

4. *Personnel screening*. Requirements for certification of water system operators are currently under review by the EPA. It might be worthwhile to consider introducing requirements for background checks into this process.

5. *Emergency planning*. Per SDWA regulations, water suppliers are required to perform emergency planning to cover instances of system disruption. However, there appears to be a need for guidance as to how, in particular, to plan for sabotage-related scenarios. Development of guidance for emergency planners might be worthwhile. Such guidance could include appropriate responses to a threat of hostile action, such as:

    - Increased monitoring and sampling;
    - Increased facility security;
    - Procedures for immediate public notification through the Emergency Alert System;
    - Procedures for preventing ingestion of pollutants in the system (e.g., raising the residual chlorine levels in the water will give it an unappetizing taste and odor, indicating that it should not be drunk);
    - Alternatives to damaged system facilities (e.g., the availability of portable or backup emergency treatment technologies from other systems in the area); and
    - Alternative water supply strategies.

6. *Mechanisms for regulatory change.* The regulatory scheme for drinking water is relatively conducive to making regulatory amendments from the top down. Any regulation adopted by the EPA must be adopted by all states that have primary enforcement responsibility within two years of the date of promulgation of the federal regulation. The state regulations become applicable to all regulated water systems within the state, and if correctly worded, can be required to be codified in governmental water supply systems' ordinances, rules, or regulations. The water supply industry also has an appropriate forum for regulatory change; AWWA is a nationwide association that provides an information network that reaches most water supply companies, participates in EPA and state rulemakings on a regular basis, and publishes water supply system standards that are often incorporated into state construction permits or regulations.

9 EMERGENCY SERVICES INFRASTRUCTURE

9.1 General Description of Regulation

9.1.1 The Current Regulatory Environment

Overview of Emergency Services Organizational Structure

Emergency services consist of local, state, federal, and private response organizations. Local emergency services consist primarily of a very widely distributed network of local police, fire, emergency management, and emergency medical personnel. The wide distribution of responders allows for quick response. In virtually any emergency situation, the first responders at the scene will be local personnel, and they will continue to provide the main part of the response for at least the first several hours. As time progresses, depending on the nature of the emergency, local and state officials may call upon neighboring jurisdictions, the federal government, and private response organizations for assistance. If criminal activity is suspected, the U.S. Department of Justice (DOJ) may take over the primary investigatory role.

Local Response

The key players in local emergency response are generally fire and law enforcement departments. Emergency medical response in the field is provided by local fire departments (Emergency Medical System [EMS] units) and other public and private ambulance companies, in cooperation with local hospitals. Most large municipalities, counties, and states also have an emergency management agency (EMA) that performs disaster planning and provides operational oversight and coordination of response efforts in large-scale emergencies.

Local governments also have a host of local support organizations that they can call upon for assistance. Resources may be requested from other government agencies, such as public works departments, and from volunteer organizations such as local American Red Cross (ARC) chapters, Radio Amateur Civil Emergency Services (RACES), and other community service and charitable organizations. The volunteer organizations typically have both local chapters and a national umbrella organization.

State Response

Each state has an emergency management statute that lays out state-level policy and authority for emergency response. This statute lays out procedures by which the governor is authorized to declare a state of emergency, thereby acquiring special emergency powers. During the state of emergency, the governor may direct action by all state personnel, commandeer property, set curfews, order evacuations, and otherwise take all steps necessary to respond to the event without

going through the usual channels and procedures. Implementation of state-level emergency services is generally coordinated by the state EMA. This agency is usually tasked by statute with preparation and implementation of state-wide emergency planning, including coordination with local emergency services, neighboring states, and the federal government. Other major participants in emergency response at the state level generally include the state police and the state environmental protection agency, with support from various other state agencies such as public health and transportation. Most states have, in one department or another, units that can provide specialized response services such as monitoring for hazardous or radioactive materials.

Federal Response

At the national level, the Federal Emergency Management Agency (FEMA) is the primary Federal agency responsible for disaster response. FEMA maintains the Federal Response Plan (FRP) and the Federal Radiological Emergency Response Plan (FRERP) and coordinates federal assistance in the event of a Presidential declaration of emergency. FEMA also promotes emergency planning, training and preparedness on the part of state and local governments through a variety of guidance, training programs and funding mechanisms. Other agencies play significant roles too. The Environmental Protection Agency (EPA) and US Coast Guard, as co-chairs of the National Response Team, administer the National Contingency Plan (NCP)[95], which provides for response to releases of oil and hazardous substances nationwide. DOJ conducts investigations into disasters when criminal activity is suspected as the cause. Numerous other agencies, including the DoD, provide assistance with disaster response in accordance with the above-mentioned plans.

Table 9.1 briefly outlines the structure of emergency service organizations from the local to the national level.

[95] 40 CFR 300 *et seq.*

Table 9.1: Outline of Emergency Response Organizations

Type of Organization	Local	State	National
Law enforcement	Municipal Police Department County Sheriff Department	State Police Department	U.S. DOJ • FBI • ATF
Fire fighting	Local Fire Depts. (volunteer or professional) may include: • Emergency Medical Service • Hazmat Response Unit	State Fire Marshal (arson investigations and oversight)	National Fire Academy National Fire Protection Association (NFPA)
Medical	Local EMS (Fire Dept. unit) Private Ambulance Co.s Hospitals (Public/Private)	State Public Health Department	U.S. Dept. of Health and Human Services — Centers for Disease Control
Emergency Management	Municipal and County Emergency Management Departments	State EM Department	FEMA
Technical Support	Municipal/County Agencies with support roles, e.g. Public Works, Social Services Local chapters of ARC, RACES and other volunteer org'ns.	State Agencies with support roles — e.g. Public Health Dept., Highway Dept. State chapters of volunteer organizations.	Federal Agencies cooperating under the NCP, FRP, and FRERP

Physical infrastructure of Emergency Services

The physical infrastructure for emergency services includes the facilities and equipment used by the agencies that provide emergency services, and the facilities and equipment of public communications systems (e.g., radio broadcast stations) that are used to notify and instruct the public about the emergency situation. More concretely, the infrastructure includes police and fire stations, emergency operations centers, hospitals, telecommunications and data centers, radio and telephone systems used for communications among emergency workers, vehicles used by emergency workers, and radio and telephone station studios and transmission equipment.

Regulation of Emergency Services.

Regulation of emergency services differs significantly from regulation of other infrastructures, since emergency services are primarily provided by governmental entities. Regulation of electric and gas utilities, telecommunications, banking and transportation has traditionally sprung from a perceived need to balance the providers' profit motive against public goals such as safety, universal service and reasonable pricing. Emergency services, on the other hand, are mainly provided by local governments and so are presumed to operate in the public interest; there is not the same kind of tension between public and private interests of the sort that has led to extensive regulation in other areas. The conduct of emergency services is controlled through political channels in the same manner as other governmental services.

Although not as all-encompassing as those controlling other types of infrastructure, there are regulations that affect how emergency services are provided. Some of these regulations set standards for certain technical aspects of response, such as medical treatment. Others represent procedures promulgated by response agencies, detailing how they will carry out their response actions. The following areas capture the most significant emergency services-related regulations:

- Implementation of federal response. Regulations and plans issued by FEMA and the EPA determine in detail how federal disaster-response efforts are conducted.

- Implementation of state response. State EMAs issue their own regulations setting out roles, authorities, and policies for state and local response.

- Hazardous material and radiological response. Federal regulations play a significant role in preparedness for specialized response capabilities such as hazardous material (hazmat) and radiological response.

- Communications. Federal Communications Commission (FCC) regulations significantly affect the way in which public safety communications are conducted.

- Medical response. Provision of emergency medical services, like all medical services, is closely regulated at the state level.

Details of these regulatory roles are discussed in Section 9.2.2 below.

Several nongovernmental organizations publish guidance on practice and performance standards related to the infrastructure for emergency services. One example is the American Society for Testing and Materials which has published several standard guides addressing emergency medical services (communications, vehicles, dispatch, and 911 enhanced telephone systems). Another example is the National Fire Protection Association, which publishes guides related to fire protection. Some of its guides, such as *Installation, Maintenance, and Use of Public Fire Services Communications Systems*, are relevant to emergency services infrastructure.

9.1.2 Current Trends in Regulation

The major recent trend in regulation of emergency services has been the growth of specialized programs aimed at technological hazards. Following the Three Mile Island accident in 1979, FEMA and the Nuclear Regulatory Commission (NRC) established regulatory standards for emergency preparedness at nuclear power plant sites. (10 CFR 50, App. E and 44 CFR 350 *et seq.*) Those regulations apply to both nuclear utilities and the communities surrounding the plants. Shortly thereafter, the Comprehensive Environmental Response, Compensation and Liability Act of 1980 (CERCLA) established a federal response program for oil and hazardous materials spills. Following the chemical-release disasters in Bhopal, India, and Institute, West Virginia, this program was supplemented by the Emergency Planning and Community Right-To-Know Act of 1986 (EPCRA), which established requirements for local and state level hazmat preparedness programs.

9.2 Description of Selected Regulatory Agencies

9.2.1 Selection Method

FEMA and the EPA are discussed below because of the roles they play in federal planning and in promoting preparedness on the part of state and local government and industry. The FCC is discussed because of its oversight of the Emergency Alert System and its role in assigning frequencies to various kinds of public safety and other emergency radio networks. At the state level, Illinois was selected as an example of a state with a well-developed system of regulations governing emergency operations and medical response. Regulations of the Illinois Emergency Management Agency (IEMA) and the Illinois Department of Public Health (IDPH) are profiled. Lastly, the Association of Public-Safety Communications Officials (APCO) is profiled because of its role in setting standards for emergency communications.

9.2.2 Agency Descriptions

9.2.2.1 Federal Emergency Management Agency

FEMA is the federal agency with jurisdiction over the distribution of disaster relief and over emergency planning and preparedness. FEMA has carried out these responsibilities through publication of regulations and guidance. Some of the most significant are:

- Stafford Act planning and regulations. The Robert T. Stafford Disaster Assistance and Emergency Relief Act (42 U.S.C.A. § 5121 *et seq.*) authorizes federal assistance in the event of a disaster or emergency to save lives and protect public health, safety and property. The Federal Response Plan (FRP), developed and published by FEMA in coordination with 27 other agencies and departments, lays out policies and procedures for provision of this assistance. FEMA is the primary agency for receiving disaster notification and initiating response measures. The FRP includes function-specific annexes addressing specific types of assistance, including among others transportation, communications, public works and engineering, firefighting, mass care, health and medical services, urban search and rescue, and hazardous materials response. A Terrorism Incident Annex was added in February 1997, describing coordinated arrangements among FEMA, DOJ, U.S. Department of Defense (DOD), U.S. Department of Energy (DOE), EPA, and U.S. Department of Human Health and Services (DHHS).

  Also under the Stafford Act, FEMA has published detailed regulations (44 CFR 206 *et seq.*) describing the process by which governors may apply for a Presidential emergency or disaster declaration. Such declarations authorize use of federal resources for response and financial assistance for reimbursement of state and local response expenses, repair of infrastructure, and aid to individuals affected by the disaster.

- Radiological emergency preparedness. FEMA reviews and approves state and local emergency plans and preparedness for addressing the offsite effects of a radiological emergency at a commercial nuclear power plant, including evaluation of biennial exercises. Standards for this activity are published at 44 CFR 350 *et seq.* FEMA and the NRC have also issued joint guidance on this topic: NUREG-0654/FEMA-REP-1, Rev. 1, *Criteria for Preparation and Evaluation of Radiological Emergency Response Plans in Support of Nuclear Power Plants.*

- FEMA's responsibilities also include providing instructions and technical guidance on emergency preparedness to states and their political subdivisions. To that end, FEMA has issued numerous guidance documents, memoranda and letters providing specific advice and assistance in dealing with various kinds of emergencies.

9.2.2.2 Environmental Protection Agency

The EPA has had a significant role in developing and promoting preparedness against hazardous material releases. EPA regulations have driven development of hazmat response capabilities among a broad spectrum of organizations, as detailed below.

- The National Contingency Plan (NCP) (40 CFR 300) implements CERCLA, laying out procedures for federal response to spills of oil or hazardous substances. Many parts of the NCP are concerned with remediation and cleanup of sites that were contaminated long ago; however, there are also sections on immediate response to current spills. Under the NCP, certain types of spills must be promptly reported to the National Response Center, the single point of contact for the national response team (NRT). The Center immediately relays the notification to the appropriate predesignated federal on-scene coordinator (OSC),[96] who coordinates, directs and reviews the response effort in compliance with the NCP and the regional response plan for that area. The response may include assistance from other federal agencies according to their expertise. The NRT has representatives from almost every federal agency.[97] The 10 RRTs also have representatives from governor-designated state emergency response agencies.

- EPCRA regulations require preparedness against releases of "extremely hazardous substances" (EHSs) that pose particular danger to surrounding communities (40 CFR 355). The regulations direct states to set up state-level and local-level planning bodies to prepare against this hazard. Firms that use EHSs must offer assistance with this planning, and must immediately notify local authorities in the event of a release. The EPCRA regulations also require routine reporting of information such as stockpiles of EHSs and normal (non-emergency) releases (40 CFR 372).

- The EPA also has incorporated emergency preparedness provisions into several environmental regulations affecting industries that use hazardous materials. Regulations issued under the Resource Conservation and Recovery Act (RCRA) (applying to facilities that store or process hazardous waste [40 CFR 265.56]), Clean Air Act (CAA) (release prevention and response for hazardous air pollutants [40 CFR 68; 61 FR 31668, June 20, 1996; 61 FR 16958; and 61 FR 31730]), and Clean Water Act (CWA) (oil spill prevention and response [40 CFR 112]) all contain provisions addressing emergency preparedness. Under these regulations, facilities with permits for handling hazardous materials are required to have contingency plans in place; train employees on emergency response procedures; and have systems for providing warnings to employees and local

[96] The OSC is a federal official who oversees the response. The OSC will be from the Coast Guard for all oil discharges to waters, or the EPA for all discharges or releases threatening inland areas, or from DOD or DOE for releases from facilities within their jurisdiction, custody or control.

[97] In addition to the EPA and Coast Guard, the NRT has representatives from FEMA, DOJ, DOD, U.S. Department of Interior (DOI), U.S. Department of Commerce (DOC), U.S. Department of Agriculture (USDA), Department of Labor (DOL), DOE, U.S. Department of State (DOS), Research and Special Projects Administration (RSPA), NRC and DHHS.

authorities in the event of a spill.

9.2.2.3 Federal Communications Commission

The FCC was established by the Communications Act of 1934.[98] It has regulatory authority over many aspects of communications systems that serve the public, such as radio broadcast stations, television broadcast systems, and cable systems. The significance of the FCC for emergency services resides in (1) its oversight of the Emergency Alert System (EAS) for notifying and instructing the public; (2) its authority to assign frequency bands for public safety radio services; and (3) its authority to license special emergency radio services. "Public safety radio" includes the activities of local government radio, police radio, fire radio, highway maintenance, forestry-conservation radio, and emergency medical radio. "Special emergency radio services" includes the activities of medical services, rescue organizations, disaster relief organizations, school buses, and beach patrols. The FCC has established a new National Advisory Committee to provide coordination and direction in implementating the new rules and regulations for the EAS.

- Regulations pertaining to public safety radio services are found at 47 CFR 90. They lay out allowable frequencies, power output, and other technical specifications for radio equipment used by local and state public safety services.

- Requirements for the EAS are found in 47 CFR Parts 0, 11, 73 and 76. Essentially all radio and TV broadcast stations and cable providers are required to participate in the national system. Participation in state and local systems (i.e., agreeing to transmit emergency messages originating at the state or local level) is voluntary. A redundant network is set up such that the failure of any one station will not cause other area stations to miss the message. Codes and protocols for activation are provided for.

  The new regulations require participating stations to phase in upgrades to their equipment. The new equipment will allow improvements in the system; for example, it will be possible to incorporate equipment in ordinary television sets so that they turn on automatically when there is an alert signal, similar to the way National Oceanographic and Atmospheric Administration (NOAA) weather radios work now.

9.2.2.4 Illinois Emergency Management Agency

State-level emergency management in Illinois is coordinated by the Illinois Emergency Management Agency (IEMA), pursuant to the Illinois Emergency Services and Disaster Agency Act of 1975. IEMA regulations appear in Title 29 of the Illinois Administrative Code. Those regulations include:

[98] 48 Stat. 1064.

- Radiological Protection (Part 320). This part includes policy for the development and maintenance of a radiological protection program, specifications and procedures for testing and maintenance of radiological monitoring equipment, and standards and procedures for radiological training and recordkeeping.

- Individual and Family Grant Program (Part 410) and Public Disaster Assistance Program (Part 420). These parts lay out procedures for administering disaster-relief programs, in coordination with FEMA, to provide financial assistance to individuals, families, and local governments affected by disasters.

- Emergency and Written Notification of an Incident or Accident Involving a Reportable Hazardous Substance (Part 430). This part requires notification of IEMA whenever there is a reportable release of an extremely hazardous substance (as defined in EPCRA). IEMA serves as the point of contact for the State and in turn notifies other Illinois agencies as appropriate.

- Development, Annual Review, Coordination of Chemical Safety Contingency Plans (Part 610) and Emergency Planning and Community Right-to-Know (Part 620). These parts establish requirements and procedures for coordination between businesses and local governments regarding planning for hazardous material response, inventory reporting, release reporting, and emergency notifications.

- Emergency Services and Disaster Agencies: Establishment, Accreditation, and Workers' Compensation (Part 1300). This part requires establishment of local emergency services agencies by each county and by each municipality with more than 500,000 residents. It also sets standards for their accreditation and provides workers' compensation coverage for workers and volunteers engaging in emergency response activities, drills or exercises.

- Emergency Management Assistance Program (Part 1310) This part establishes administrative procedures and requirements for local emergency service agencies to receive financial assistance (grants) distributed by FEMA through the State of Illinois.

9.2.2.5 Illinois Department of Public Health

The Illinois Department of Public Health (IDPH) licenses hospitals and emergency medical transport providers (ambulances) within the State of Illinois. Some of the major components of the IDPH regulations relating to emergency medical services are:

- Hospital emergency room requirements. General-service hospitals are required to provide at least a minimum level of emergency care. (Some specialized hospitals, such as psychiatric hospitals, are not.) In addition, the regulations provide that facilities meeting certain additional requirements may be designated as primary and secondary Trauma Centers. The requirements at each level are extensive and include stipulations as to

equipment, supplies, staffing, 24-hour availability, and other factors.

- Emergency medical transport requirements. Each service providing emergency medical transport, including fire department emergency medical services, ambulances, watercraft, and helicopters must be licensed by IDPH. Each such service must meet extensive requirements including training and certification of personnel, availability of medical equipment and supplies for enroute care, communications capabilities, and other factors.

- Emergency medical systems. The IDPH regulations establish emergency medical service regions and provide for a hierarchy of coordinated services within each region. Within each region, the primary resource hospital oversees and directs the delivery of emergency medical services performed by the transport providers and other participating hospitals.

9.2.2.6 Association of Public-Safety Communications Officials

The objectives of the Association of Public-Safety Communications Officials (APCO) are to foster the development and progress of the art of public safety communications; ensure greater cooperation in the correlation of the work and activities of town, county, state and federal agencies; promote cooperation between these agencies and the FCC; and conduct surveys, management and training seminars. APCO reviews and approves proposed practice and performance standards developed by organizations such as the American Society for Testing and Materials. It has recently participated in developing APCO-25, a suite of standards on digital radio communications that is intended to improve the effectiveness and reliability of intraagency and interagency public safety radio communications.

9.3 Regulations and Critical Infrastructure Protection

9.3.1 Impact of the Regulations on Protection of Critical Infrastructure

The security of the emergency services infrastructure appears to be little affected by regulation. As noted earlier, regulation of emergency services is not pervasive; and among these regulations, few are concerned with the security of associated infrastructure. It should be noted, however, that the infrastructure of emergency services is decentralized and inherently resilient against attack. To keep response times short, police and fire services are provided out of numerous local stations. In a large city, there will be dozens or hundreds of stations. An attack on any one (or even several) of these locations cannot disable the entire response system. An attack on a police station will not even completely disable that station's personnel, since at any given time a large fraction of police officers are out on patrol. In addition, police and fire personnel are somewhat less vulnerable than most in that they have protective equipment on hand, and in the case of police at least can defend themselves against armed attack.

Emergency medical services and hospitals are also decentralized. Urban areas typically have several hospitals with emergency care capability within close range, as well as numerous

transport services.

The strongest connection between regulation and emergency service infrastructure assurance appears to be in the area of communication to the public. The FCC's EAS system regulations establish network redundancies, passwords, testing mechanisms, and other measures directly intended to make the EAS more robust and less subject to single-point failure.

The regulation of emergency services *has* affected the ability of those services to respond to the types of emergencies that the Commission is concerned with. This has occurred through two mechanisms: one, coordinated planning for federal response, and two, the establishment of a network of public and private capabilities for response to emergencies involving hazardous or radioactive materials.

Coordinated Planning for Federal Response.

The development of emergency planning at the federal level, including the FEMA Stafford Act regulations, NCP, FRP, and FRERP, has strengthened response capabilities for major disasters of all types. These plans have been extensively verified through exercises and lessons learned from actual responses. Implementation of these plans has enhanced federal response capabilities. Also as a result of these plans, state and local governments are now in the habit of promptly notifying federal officials when major emergencies occur, and they routinely request assistance when it appears that local resources will be exhausted. This means that in the event of a significant terrorist event, local response officials could be expected to provide notice to key federal agencies within a matter of minutes. The resultant federal response will be well coordinated and will proceed according to established protocols for assistance to local officials.

Network of Hazmat/Rad Response

Regulations adopted since 1980 have created a network of public and private capabilities for response to radiological and hazardous material emergencies. EPA environmental regulations implementing EPCRA, RCRA, and CAA require firms that handle or store hazardous materials to have emergency preparations in place. Such firms are required to have in-house emergency response organizations, emergency plans, training programs, procedures for giving prompt warning to employees in the event of an emergency, and, if necessary, a method of notifying off-site authorities of the need to evacuate nearby areas. They are also required to promptly notify local and federal officials when there is a release of hazardous materials.

The EPCRA regulations set up a network of local and state emergency response organizations specifically to plan for and implement response to hazardous material emergencies. Each state has a state emergency response commission (SERC) to implement preparedness statewide, and local emergency planning committees (LEPCs), usually at the county or municipal level, to perform local planning functions. The LEPCs generally consist of officials from local response agencies and may also include industry representatives. Firms that store or use regulated

hazardous materials are required to offer assistance and information to their local LEPCs. Thus, as a result of the EPCRA regulations, there is now a national network of state and local hazardous materials response agencies. These agencies in turn participate as state and local representatives on the RRTs under the NCP.

Radiological response capabilities are also relatively widespread, partly as a result of the regulation of nuclear power plants. Regulations adopted by the NRC and FEMA require radiological emergency response capability on the part of nuclear utilities and communities where nuclear power plants are located. Over 40 states, as well as numerous localities, participate in this program. They are required to have radiological emergency response plans, including the ability to assess radiological hazards and implement appropriate protective measures for the public.

One other agency also bears mention in this respect. The Occupational Safety and Health Administration (OSHA) administers regulations on workplace safety. Pursuant to EPCRA, in 1987 OSHA adopted regulations governing the safety of emergency response personnel who respond to hazardous material incidents (29 CFR §1910.120(q)). Partly as a result of these regulations, hazmat response teams across the country are trained and equipped to operate in hazardous environments with appropriate personal protective gear.

9.3.2 Measures for Improvement

Review of the regulations described above, along with conversations with emergency response officials, indicates that the primary opportuniy for improvement of response capabilities lies in enhancement of emergency communications. Two significant measures are already being undertaken. First, the FCC has instituted improvements in the EAS to increase speed and reliability of transmission of public instructional messages. The older Emergency Broadcast System (EBS) used a "daisy chain" of transmissions from a single primary entry station. If any link in the transmission was severed, the stations beyond the break would not receive the transmissions. Under EAS, a state is divided into regions, and each region has two primary entry stations that are continuously monitoring state emergency broadcast frequencies and each other. Other stations within the region monitor these stations. Thus EAS is a parallel system, with redundancies that make it more resilient against breakdown or attack.

The second measure that has been the adoption of technical standards for design of the next generation of communications equipment. Emergency service organizations and communications equipment manufacturers have cooperated to set standards to improve the effectiveness and reliability of public-safety communications equipment. They developed APCO 25, a suite of standards for digital radio communications for public safety applications that improves interoperability and talk-around capabilities (APCO-25 also refers to the process that developed these standards). Interoperability refers to the ability to use components made by different manufacturers in a single system. Talk-about refers to the capability to have portable-to-portable and/or mobile-to-mobile intercommunication without the use of a repeater. This is particularly valuable for tactical operations involving different agencies. Organizations

representing governmental public safety radio users at each level of government (Association of Public Safety Communications Officials, National Association of State Telecommunications Directors, Department of Defense, National Telecommunications and Information Administration) and industry organizations (Telecommunications Industry Association, American National Standards Institute) participated in the APCO-25 process.

The action that remains to be taken is allocation of additional radio spectrum for use by emergency response agencies. The APCO-25 process will allow development of equipment that uses narrower radio bandwidths for communications. This will effectively double the number of channels available to public safety organizations. However, the scarcity of available channels remains an issue with emergency service organizations. Many such organizations are advocating reallocation of a portion of the radio spectrum that is currently reserved for television to public-safety radio communications. Such a reallocation would effectively double the available number of channels again. A bill to require the FCC to set aside an additional 24 MHz of radio spectrum for public safety was introduced in the Senate in February 1997 (S. 255, Law Enforcement and Public Safety Telecommunications Empowerment Act). This bill is currently inactive; however, similar language has been incorporated into the Senate version of the Budget Reconciliation Act (S. 947, A Bill to Provide for Reconciliation Pursuant to Section 104(a) of the Concurrent Resolution on the Budget for Fiscal Year 1998, June 23, 1997).

[This page intentionally left blank.]

APPENDIX

ACRONYMS, AGENCIES AND ASSOCIATIONS, STATUTES AND REGULATIONS

Acronyms

ALM	-	automatic loan machines
ATM	-	automatic teller machine
BBS	-	bulletin board system
CFR	-	Code of Federal Regulations
CNG	-	compressed natural gas
EAS	-	Emergency Alert System
EDI	-	electronic data interchange
EFT	-	electronic funds transfers
EHSs	-	extremely hazardous substances
EOC	-	emergency operating center
EWGs	-	exempt wholesale generators
FR	-	Federal Register
FRERP	-	Federal Radiological Emergency Response Plan
FRP	-	Federal Response Plan
IAC	-	Illinois Administrative Code
IFR	-	instrumental flight rule
INFOSEC	-	information security
ISO	-	independent system operator
LDC	-	local distribution company
LEPC	-	Local Emergency Planning Committee
LNG	-	liquefied natural gas
LPG	-	liquefied petroleum gas
MCL	-	maximum contaminant level
NCP	-	National Contingency Plan
NCS	-	National Communications System
NRT	-	National Response Team
OASIS	-	Open Access Same-time Information System
OCS	-	outer continental shelf
OPSEC	-	operational security
OSC	-	on-scene coordinator
PSN	-	public switched network
PUC	-	public utility commission
QFs	-	qualifying facilities

Acronyms Cont'd

RDC	-	residual disinfectant concentration
RSU	-	remote service units
SCADA	-	supervisory control and data acquisition
SERC	-	State Emergency Response Commission
SPR	-	Strategic Petroleum Reserve
SYSEC	-	system security
TAC	-	Texas Administrative Code
USC	-	United States Code
USCA	-	United States Code Annotated
VASI	-	visual approach slope indicator
VOR	-	very-high-frequency omni-range

Agencies and Associations

AEC	-	Atomic Energy Commission
AGA	-	American Gas Association
APCO	-	Associated Public Safety Communications Officers
API	-	American Petroleum Institute
AWWA	-	American Water Works Association
BLM	-	Bureau of Land Management
DOC	-	Department of Commerce
DOD	-	Department of Defense
DOI	-	Department of Interior
DOJ	-	Department of Justice
DOL	-	Department of Labor
DOS	-	Department of State
DOT	-	Department of Transportation
EPA	-	Environmental Protection Agency
ERDA	-	Energy Research & Development Administration
FAA	-	Federal Aviation Administration
FCC	-	Federal Communications Commission
FDIC	-	Federal Deposit Insurance Corporation
Fed	-	Federal Reserve System/Board
FERC	-	Federal Energy Regulatory Commission
FFIEC	-	Federal Financial Institutions Examination Council
FHFB	-	Federal Housing Finance Board
FHWA	-	Federal Highway Administration
FPC	-	Federal Power Commission
FRA	-	Federal Railroad Administration
FTA	-	Federal Transit Administration

Agencies and Associations Cont'd

GRI	-	Gas Research Institute
ICC	-	Illinois Commerce Commission
ICEC	-	Illinois Commission on Electronic Commerce
IDOT	-	Illinois Department of Transportation
IDPH	-	Illinois Department of Public Health
IEEE	-	Institute of Electronics and Electric Engineers
IEMA	-	Illinois Emergency Management Agency
IEPA	-	Illinois Environmental Protection Agency
INGAA	-	Interstate Natural Gas Association of America
IPCB	-	Illinois Pollution Control Board
MMS	-	Mineral Management Service
NAC	-	National Advisory Committee (FAA)
NASDAQ	-	National Association of Securities Dealers' Automated Quotation System
NERC	-	North American Electric Reliability Council
NFPA	-	National Fire Protection Association
NJBPU	-	New Jersey Board of Public Utilities
NOAA	-	National Oceanographic and Atmospheric Administration
NPC	-	National Petroleum Council
NRC	-	Nuclear Regulatory Commission
NRIC	-	Network Reliability and Interoperability Council
NTIA	-	National Telecommunications and Information Administration
OCC	-	Office of the Comptroller of the Currency
OSHA	-	Occupational Safety and Health Administration
OTS	-	Office of Thrift Supervision
PUCT	-	Public Utility Commission of Texas
RSPA	-	Research and Special Programs Administration
RTC	-	Resolution Trust Corporation
SEC	-	Security and Exchange Commission
STB	-	Surface Transportation Board
TRC	-	Texas Railroad Commission

Statutes and Regulations

APSPA	-	Accountable Pipelines Safety and Partnership Act of 1996 (Pub. L. 104-304)
CA of 1863	-	Currency Act of 1863 (Chap. 106, 13 Stat. 99)
CAA	-	Clean Air Act (42 U.S.C.A. §§ 7401-7671q)
CPUC	-	California Public Utilities Code
CWA	-	Clean Water Act (33 U.S.C.A. §§ 1251-1387)
DIDMCA	-	Depository Institutions Deregulations and Monetary Control Act of 1980
ECPA	-	Energy Conservation and Production Act of 1976 (Pub. L. 94-385)

Statutes and Regulations Cont'd

EPAA	-	Emergency Petroleum Allocation Act of 1973 (Pub. L. 93-159, 87 Stat. 627)
EPACT	-	Energy Policy Act of 1992 (Pub. L. 102-486, 106 Stat. 2776)
EPCA	-	Energy Policy and Conservation Act (Pub. L. 94-163, 89 Stat. 871)
EPCRA	-	Emergency Planning and Community Right-To-Know Act of 1986 (42 U.S.C.A. §§ 11001 - 11050)
FFIRREA	-	Federal Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (Pub. L. 101-73, 103 Stat. 183)
FIRIRCA	-	Financial Institutions Regulatory and Interest Rate Control Act of 1978 (Pub. L. 95-630, 92 Stat. 3641)
FPA	-	Federal Power Act (16 U.S.C.A. § 791 *et seq.*)
FRA	-	Federal Reserve Act of 1913 (Pub. L. 63-43, 38 Stat. 251, 12 U.S.C.A. § 221)
Glass-Steagall	-	Glass-Steagall Act of 1933 (48 Stat. 162)
ILCS	-	Illinois Consolidated Statutes
IEPA	-	Illinois Environmental Protection Act (415 ILCS 5/1 *et seq.*)
IESA	-	Illinois Electric Supplier Act (220 ILCS 30/1 *et seq.*)
IGPSA	-	Illinois Gas Pipeline Safety Act (220 ILCS 20/1 *et seq.*)
IPUA	-	Illinois Public Utilities Act (220 ILCS 5/1-101 *et seq.*)
ISTEA	-	Intermodal Surface Transportation Efficiency Act of 1991 (Pub. L. 102-240, 105 Stat. 1914) (Amending 23 U.S.C.A. § 101 *et seq.*)
McFadden Act	-	McFadden Act of 1927 (Pub. L. 69-639, 44 Stat. 1224)
NBA	-	National Banking Act of 1864 (13 Stat. 99, 12 U.S.C. § 35 *et seq.*)
NGA	-	Natural Gas Act of 1938 (15 U.S.C.A. §§ 717-717z)
NGPA	-	Natural Gas Policy Act of 1978 (Pub. L. 95-621 (codified in various sections of 15 U.S.C., see especially 15 §§ 3301 *et seq.*)
NGWDA	-	Natural Gas Wellhead Decontrol Act (Pub. L. 95-617, 92 Stat. 3117)
PSA	-	Pipeline Safety Act (49 U.S.C.A. §§ 60101 *et seq.*)
PUHCA		Public Utility Holding Company Act of 1935 (15 U.S.C.A. §§ 79-79z)
PURPA	-	Public Utility Regulatory Policies Act of 1978
PURA95	-	Public Utility Regulatory Act of Texas
Riegle-Neal	-	Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994 (Pub. L. 103-328, 108 Stat. 2338)
SDWA	-	Safe Drinking Water Act (Public Health Service Act, 42 U.S.C.A. §§ 300f to 300j-26)
SA of 1933	-	Securities Act of 1933 (48 Stat. 74)
SE of 1934	-	Security Exchange Act of 1934 (48 Stat. 881)
Stafford Act	-	Robert T. Stafford Disaster Assistance and Emergency Relief Act (42 U.S.C.A. § 5121 *et seq.*)